Networking the world's business data™

EFCM Basic

EFCM Basic User Manual

P/N 620-000240-000
REV A

Simplifying Storage Network Management

McDATA Corporation
380 Interlocken Crescent Broomfield, CO 80021-3464
Corporate Headquarters: 800-545-5773
Sales E-mail: sales@mcdata.com *Web:* www.mcdata.com

Record of Revisions and Updates

Revision	Date	Description
620-000245-000	7/2005	Initial release of the manual

Copyright © 2002 - 2005 McDATA Corporation. All rights reserved.

Printed July 2005

First Edition

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written consent of McDATA Corporation.

The information contained in this document is subject to change without notice. McDATA Corporation assumes no responsibility for any errors that may appear.

All computer software programs, including but not limited to microcode, described in this document are furnished under a license, and may be used or copied only in accordance with the terms of such license. McDATA either owns or has the right to license the computer software programs described in this document. McDATA Corporation retains all rights, title and interest in the computer software programs.

McDATA Corporation makes no warranties, expressed or implied, by operation of law or otherwise, relating to this document, the products or the computer software programs described herein. McDATA CORPORATION DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE. In no event shall McDATA Corporation be liable for (a) incidental, indirect, special, or consequential damages or (b) any damages whatsoever resulting from the loss of use, data or profits, arising out of this document, even if advised of the possibility of such damages.

©2005 McDATA Corporation. All rights reserved. McDATA, the McDATA logo, McDATA Eclipse, Fabricenter, HotCAT, Intrepid, Multi-Capable Storage Network Solutions, Networking the World's Business Data, nScale, nView, OPENready, SANavigator, SANpilot, SANtegrity, SANvergence, SecureConnect and Sphereon are trademarks or registered trademarks of McDATA Corporation. OEM and Reseller logos are the property of such parties and are reprinted with limited use permission. All other trademarks are the property of their respective companies. All specifications subject to change.

Contents

Preface xv

Chapter 1 Introduction

Overview 1-1
Using the EFCM Basic Interface to Perform Tasks 1-2
Benefits 1-4
Key Terms 1-5
Fabric 1-5
Storage Area Network (SAN) 1-5
Zone (Zoning) 1-5
Zone Member 1-5
Zone Set 1-5
Suggested Reading 1-6
Where to Start 1-6
Starting the EFCM Basic Interface 1-7
Using the EFCM Basic User Interface 1-10
Navigational Tools of the EFCM Basic Page 1-11
Licensed Features 1-13

Chapter 2 Viewing Product Information

Opening the Hardware Page 2-1
Front View and Rear View 2-2
Product Information 2-3
Viewing the Port List 2-4
Port List 2-5
Port Information 2-7
Health Status Information 2-9
Transceiver Information 2-10

Viewing the FRU List 2-11
Viewing Operating Parameters 2-12
Viewing the Node List 2-14
Viewing Performance Information 2-15
Using the Performance Page 2-15
Parts of Statistics Tables 2-15
Port Utilization Percentages and Error Totals 2-16
Traffic Statistics 2-16
Error Statistics 2-17
Class 2 Statistics 2-19
Class 3 Statistics 2-19
Open Trunking Statistics 2-19

Chapter 3 Configuring the Product

Factory Default Values 3-2
Configuring Ports 3-2
Configuring Basic Port Information 3-2
Configuring Port Rx BB_Credits 3-5
Configuring NPIV 3-7
Configuring Switch Information 3-9
Configuring Switch Identification 3-9
Configuring Switch Date and Time 3-10
Configuring Switch Parameters 3-11
Configuring Fabric Parameters for the Switch 3-14
Configuring Network Parameters for the Switch 3-16
Configuring SNMP 3-18
Configuring CLI and SSH 3-19
Configuring OSMS and Host Control 3-20
Configuring SSL 3-21
Zoning 3-24
Configuring Performance Parameters 3-25
Configuring Open Trunking 3-25
Configuring Preferred Paths 3-27
Configuring Port Fencing 3-30
Setting a Switch Online and Offline 3-32
Enabling and Disabling Software 3-33
Enabling and Disabling the CLI 3-33
Upgrade Options 3-34

Chapter 4 Configuring Zoning

Understanding Zoning 4-1
Controlling Access Across a Fabric 4-2
Controlling Access at the Switch 4-5
Controlling Access at the Server or Storage Device 4-5
Zoning Concepts 4-6
Merging Zoned Fabrics 4-11
Using The Zoning Page 4-13
Creating and Modifying a Zone 4-14
Create a New Zone 4-14
Add Zones Members to a Zone 4-15
Remove Zone Members from a Zone 4-16
Save the Zone to the Zone Set 4-16
Rename a Zone 4-16
Configuring the Zone Set 4-17
Create a Zone Set 4-17
Name and Rename a Zone Set 4-18
Add Zones to the Zone Set 4-18
Delete Zones From the Zone Set 4-19
Change a Zone that is in the Zone Set 4-19
Activate and Cancel the Zone Set Changes 4-19
Deactivate the Active Zone Set 4-20
State of the Default Zone 4-20

Chapter 5 Configuring Security

Defining Authentication Settings 5-1
Configuring User Authentication 5-2
Adding, Editing, and Deleting User Names 5-2
Defining User Properties 5-4
Defining Authentication Settings for the Product 5-5
User Accounts with RADIUS Server 5-5
Configuring Software Authentication 5-6
Defining Which Software Is Authenticated 5-6
Configuring Software Authentication Properties 5-8
Configuring Out-of-Band Settings 5-8
Configuring OSMS Settings 5-9
Configuring Device Authentication 5-10
Defining the CHAP Secret of the Product 5-11
Defining Port Authentication Sequences 5-11
Configuring Authentication Devices 5-12
Applying a CHAP Secret to the Device 5-12
Adding a Device to the Authentication Devices List 5-13

Removing a Device from the Authentication Devices List5-13
Configuring Port Authentication 5-14
Configuring the IP Access Control List 5-15
Setting the IP ACL State 5-16
Adding New Members to the List 5-16
Editing the List.....5-17
Deleting Members from the List 5-17
Configuring the RADIUS Server 5-18
Add an Entry to the RADIUS Server List 5-19
Edit an Entry on the RADIUS Server List.....5-20
Delete an Entry from the RADIUS Server List.....5-20
Configure Priority of the RADIUS Servers.....5-20
Configuring the Dead Time Parameter.....5-21
Enabling the Enterprise Fabric Mode 5-22
Features and Parameters Enabled with Enterprise Fabric Mode.....5-22
Configuring Fabric Binding 5-25
Enable, Disable, and Online State Functions.....5-26
Identify Fabric Binding Status 5-27
Load the Current Fabric to the FBML 5-27
Add Members to the FBML 5-27
Delete Members from the FBML.....5-27
Activate Fabric Binding 5-28
Deactivate Fabric Binding 5-28
Configuring Switch Binding 5-29
Enable, Disable and Online State Functions.....5-30
Define Switch Binding State 5-31
Adding Members to the SBML.....5-31
Removing Members from the SBML 5-32
Configuring Port Binding.....5-33
Enabling and Disabling Safe Zoning Mode.....5-34
Upgrade Options 5-35

Chapter 6 Viewing System Logs

Viewing the Event Log 6-2
Error Event Code Categories 6-3
Viewing the Link Incident Log 6-4
Viewing the Audit Log 6-6
Viewing the Security Log 6-8
Viewing the Open Trunking Re-Route Log.....6-10
Viewing the Fabric Log.....6-12
Viewing the Embedded Port Frame Log.....6-14

Defining Filtering Settings 6-15
Viewing All Logs 6-16
Viewing Syslog Configuration 6-18
Enable and Disable Syslogs 6-19
Add a Syslog Recipient 6-19
Edit a Syslog Recipient 6-20
Delete Syslog Recipients 6-20
Specify Which Logs Are Sent to a Recipient 6-20

Chapter 7 Performing Product Maintenance

Switch Maintenance Tasks 7-2
Set the Product Online State 7-2
Set the Unit Beaconing State 7-3
Clear System Error Lights 7-3
Perform a System Configuration Reset 7-3
Setting Individual Port Beaconing 7-5
Resetting Ports 7-6
Performing Diagnostics on a Port 7-7
Accessing System Files 7-9
Retrieve the Dump File 7-9
Create the Data Collection File 7-10
Configuration Backup 7-11
Configuration Restoration 7-12
Upgrading Firmware 7-13
Activating Optional Features 7-14
Viewing Product Information 7-15
Enabling and Disabling Unit Beaconing 7-17
Clearing the System Error Light 7-18
HA Power Supplies 7-18
Upgrade Options 7-18

Chapter 8 Using the Fabric View

Overview of the Fabric View 8-1
Fabric View Elements 8-1
Fabric Tree 8-2
Product Boxes 8-3

Chapter 9 Software Upgrade and Feature Installation

Adding Licensed Features....9-2
Licensed Features....9-3
Entering a Feature Key....9-3

Chapter 10 Upgrading Your SAN Management System

Differences Between EFCM Basic and other McDATA Products .. 10-1
Enterprise Fabric Connectivity Manager....10-1
SANavigator....10-2
Features and Functions....10-3
Management Features Provided by EFCM and/or SANavigator . 10-4
Configuring the Product....10-4
Maintaining the Product....10-4
Monitoring System Performance....10-5

Appendix A Error Messages

Glossary....g-1

Index....i-1

Figures

1-1 Enter Network Password Dialog Box 1-7
1-2 Fabric View 1-9
1-3 Example EFCM Basic Page Showing a 24-Port Switch 1-10

2-1 Product Hardware Page 2-2
2-2 Port List Page 2-5
2-3 Optics Monitoring Information 2-10
2-4 FRU List Page 2-11
2-5 Operating Parameters Page 2-12
2-6 Node List Page 2-14
2-7 Product Performance Page 2-16

3-1 Port Basic Information Page 3-3
3-2 Rx BB_Credit Page 3-6
3-3 Port NPIV Configuration Page 3-8
3-4 Switch Identification Page 3-9
3-5 Switch Date and Time Page 3-10
3-6 Switch Parameters Page 3-11
3-7 Fabric Parameters Page 3-14
3-8 Switch Network Configuration Page 3-17
3-9 SNMP Configuration Page 3-18
3-10 CLI Configuration Page 3-20
3-11 OSMS Configuration Page 3-21
3-12 SSL Configuration Page 3-24
3-13 Open Trunking Page 3-26
3-14 Preferred Path Page 3-29
3-15 Port Fencing Page 3-31
3-16 Configure Menu 3-33

4-1 Zoning through a Single Fibre Channel Managed Product 4-3
4-2 Zoning Through a Multiswitch Fabric 4-4
4-3 Zoning Page 4-13

5-1 User Authentication Configuration Page 5-3
5-2 Software Authentication Configuration Page 5-7
5-3 Device Authentication Configuration Page 5-10
5-4 Port Authentication Configuration Page 5-14
5-5 IP Access Control List 5-15
5-6 RADIUS Server Page 5-19
5-7 Enterprise Fabric Mode Page 5-22
5-8 Fabric Binding Page 5-26
5-9 Switch Binding Page 5-30
5-10 Port Binding Page 5-33
5-11 Security Menu 5-34

6-1 Event Log Page 6-2
6-2 Link Incident Log Page 6-4
6-3 Audit Log Page 6-6
6-4 Security Log Page 6-8
6-5 Open Trunking Re-Route Log Page 6-10
6-6 Fabric Log Page 6-13
6-7 Embedded Port Frame Log Page 6-14
6-8 All Logs Page 6-16
6-9 Syslog Configuration Page 6-18

7-1 Switch Maintenance Page 7-2
7-2 Ports Beacon Page 7-5
7-3 Port Reset Page 7-6
7-4 Port Diagnostics Page 7-7
7-5 Port Diagnostics - Executing Page 7-8
7-6 System Files Page 7-9
7-7 Selecting the Location to Save the CTP Maintenance Information 7-10
7-8 Backup Configuration Page 7-11
7-9 Restore Configuration Page 7-12
7-10 Firmware Upgrade Page 7-13
7-11 Product Information Page 7-15
7-12 Maintenance Menu 7-17

8-1 Fabric View with 10 Domain IDs 8-2

9-1 Maintenance Feature Installation Page 9-2

Tables

1-1 Items on the Tool Bar 1-11
1-2 Items on the Menu Bar 1-12
1-3 Items Used in Multiple Pages 1-12

2-1 Status Indicators 2-3

4-1 Zone Set Configuration 4-10
4-2 Merging Zones 4-12

6-1 Facility Code Levels 6-19

Preface

This publication provides instructions on using the McDATA® EFCM Basic® interface to configure, operate, and monitor a Storage Area Network (SAN).

Who Should Use This Manual

This publication is intended for data center administrators, LAN administrators, operations personnel, and customer support personnel who administer user access to this application and monitor and manage product operation.

Organization of This Manual

This publication is organized as follows:

- Chapter 1, *Introduction* provides an overview of the EFCM Basic interface and instructions for logging into EFCM Basic.
- Chapter 2, *Viewing Product Information* describes how to view hardware, port, and node information for the product, as well as the product's operating parameters.
- Chapter 3, *Configuring the Product* describes how to configure port, switch, network, and performance parameters for the product.
- Chapter 4, *Configuring Zoning* provides an overview of zoning and how to create zones for a simple SAN.
- Chapter 5, *Configuring Security* describes how to configure security for the product. This includes login and authentication configuration.
- Chapter 6, *Viewing System Logs* describes how to monitor product and port performance, and access information useful for troubleshooting problems.

- Chapter 7, *Performing Product Maintenance* provides procedures to perform various maintenance tasks for the product.
- Chapter 8, *Using the Fabric View* describes how to use this option to configure and view a small fabric.
- Chapter 9, *Software Upgrade and Feature Installation* describes functionality related to upgrading your system using EFCM Basic licensed features or switching to a SAN Management System more appropriate to a large SAN.
- Chapter 10, *Upgrading Your SAN Management System* describes reasons to consider migrating from EFCM Basic to the Enterprise Fabric Connectivity Manager (EFCM) or SANavigator™.
- Appendix A, *Error Messages* provides a list of error messages that are displayed by EFCM Basic, as well as reasons for the error messages and possible solutions.
- The *Glossary* defines terms, abbreviations, and acronyms used in this manual.
- An *Index* is also provided.

Related Documentation

McDATA switch or director user manuals provide information about Fibre Channel products. Other publications that may prove helpful include:

- *Configuration Backup and Restore Utility Installation and User Guide* (958-000370)
- *McDATA Products in a SAN Environment Planning Manual* (620-000124)
- *McDATA SNMP Support Manual* (620-000131)
- *McDATA Enterprise Operating System Command Line Interface User Manual* (620-000134)
- Each McDATA product has a product installation and service manual. Ensure that you have the product installation and service manual that came with the product.

Opening Online Help

To open online help for the EFCM Basic interface, click on the Help link in the EFCM Basic navigation panel.

Manual Conventions

The following notational conventions are used in this document:

TIP: A tip presents useful information about the tasks being described, such as a shortcut.

NOTE: A note presents important information that is not hazard-related.

ATTENTION! An attention notice presents important information about activities that could result in loss of equipment function or loss of data.

Where to Get Help

For technical support, end-user customers should call the phone number located on the service label attached to the front or rear of the hardware product.

McDATA's "Best in Class" Solution Center provides a single point of contact for customers seeking help with McDATA software products. The Solution Center will research, explore, and resolve inquiries or service requests regarding McDATA products and services. The Solution Center is staffed 24 hours a day, 7 days a week, including holidays.

NOTE: To expedite warranty entitlement, please have your product serial number available.

McDATA Corporation

380 Interlocken Crescent

Broomfield, CO 80021

Phone: **(800) 752-4572** or **(720) 558-3910**

Fax: (720) 558-3851

E-mail: support@mcdata.com

NOTE: Customers who purchased the hardware product from a company other than McDATA should contact that company's service representative for technical support.

Forwarding Publication Comments

We sincerely appreciate any comments about this publication. Did you find this manual easy or difficult to use? Did it lack necessary

information? Were there any errors? Could its organization be improved?

Please send your comments via e-mail, our home page, or FAX. Identify the manual, and provide page numbers and details. Thank you.

E-mail:	pubsmgr@mcdata.com
Home Page:	http://www.mcdata.com
FAX:	Technical Communications Manager (720) 558-8999

Ordering Publications

To order a paper copy of this manual, contact your McDATA representative, or use the contact information listed below.

Phone: (800) 545-5773 and select the option for information on our complete family of enterprise-to-edge SAN solutions.

Fax: (720) 558-4193

Trademarks

The following terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of McDATA Corporation in the United States, other countries, or both:

Registered Trademarks	Trademarks
Fabricenter®	E/OS™
HotCAT®	Eclipse™
Intrepid®	Fibre Channel Director™
McDATA®	OPENconnectors™
OPENready®	SANvergence™
SANavigator®	Sphereon™
SANtegrity®	EFCM Basic™

All other trademarked terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of their respective owners in the United States, other countries, or both.

1 Introduction

The following sections provide an introduction to the EFCM® Basic application solution:

- *Overview* *1-1*
- *Benefits* *1-4*
- *Key Terms* *1-5*
- *Suggested Reading* *1-6*
- *Where to Start* *1-6*
- *Starting the EFCM Basic Interface* *1-7*
- *Using the EFCM Basic User Interface* *1-10*

Overview

The EFCM Basic solution is a web-based graphical user interface (GUI), based on HTML, that enables you to administer products, monitor products and ports, and perform tasks to manage a simple Storage Area Network (SAN). You can also use EFCM Basic to perform troubleshooting tasks and upgrade product firmware.

With product firmware E/OS 8.0 (or later) installed, administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the product through the EFCM Basic interface.

The EFCM Basic interface supports product configuration, statistics monitoring, and basic operations. The EFCM Basic interface neither replaces nor offers all of the management capability of the EFC Manager (EFCM) application and its Element Manager applications.

(For example, the EFCM Basic interface does not support all product maintenance functions.)

In addition, the EFCM Basic interface provides hyperlink access to other products in a fabric, which means those products can also be managed. Refer to Chapter 10, *Upgrading Your SAN Management System* for information on differences between the EFCM Basic interface and other applications such as EFCM and SANavigator.

Using the EFCM Basic Interface to Perform Tasks

Users can perform the following tasks using the EFCM Basic interface:

- Display the properties and operational status of the product, FRUs, and Fibre Channel ports, display product operating parameters, and display fabric parameters.
- Configure the director or switch, including:
  - — Fibre Channel port parameters, port types, and data transmission speeds.
  - — Product identification, date and time, operating domain parameters, fabric parameters, and network addresses.
  - — Parameters for product management through Simple Network Management Protocol (SNMP), the Command Line Interface (CLI), the Open System Management Server (OSMS) feature, or the Fibre Connection (FICON™) management server (FMS) feature.
  - — Security options which include authorized users, settings, port binding, switch binding, and fabric binding. Additional security includes setting access to IP ACL, Authorization, and RADIUS functions.

NOTE: The ES-1000 Switch, and loop devices do not support out-of-band management through FMS. However, these switches do support transmission of FICON frames.

  - — Zones and zone sets.
  - — Authentication for users.
- Monitor ports, port optics, and port statistics, and display the event log and node list.

- Perform product operations and maintenance tasks, including:
  - — Enable unit beaconing, turn off the system error light, set the product online or offline, and perform a configuration reset.
  - — Enable port beaconing, perform port diagnostics, and reset ports.
  - — Retrieve dump files and retrieve product information files.
  - — Install optional feature keys.
  - — Configure product Internet Protocol (IP) addresses, names, and SNMP settings.
  - — Install new versions of product firmware.
  - — Manage user access to features.
  - — Control product ports on an individual basis.
  - — Troubleshoot problems using event log and error status indicators. Administrators and operators can access real-time information about the product and fabric.

The EFCM Basic interface requires an industry standard web browser of release level 4.0 or higher supporting HTML version 4.0 and JavaScript version 1.0. For optimum results, the use of Microsoft's Internet Explorer 6.x or Netscape Navigator 7.x or higher is recommended. The browser software should be compliant with HTML 4.0 and Javascript 1.0 for full functionality, optimum performance, and best appearance.

At the web browser, the user enters the IP address of the product as the Internet uniform resource locator (URL). When prompted at a login screen, the user enters a user name and password.

NOTE: The default user name is **Administrator** and the default password is **password.** The user name and password are case-sensitive. After the initial log on, you will need to change the password for the Administrator.

Benefits

The EFCM Basic interface provides users the following benefits:

- EFCM Basic enables a single product to be managed from a single point of access. An administrator can manage a product from any location (such as their office, a raised floor area, or a conference room) within the company's public/private networks. When an administrator accesses the product, the most current information about that product is presented (and refreshed as needed) to the administrator. This easy access provides a single point of product administration that is not limited to the location of an application or special hardware.
- Ability to perform tasks is protected through authorization based on user roles that are defined as operators and administrators. This enables companies to decide who should perform everyday tasks (such as monitoring product status) and sensitive tasks (such as installing firmware updates). This flexible approach enables companies to define roles within their organization while providing a level of security against unauthorized access.
- No installation is required because the EFCM Basic interface is part of the product. By simply starting a web browser and entering the network address of the product and logging into it, EFCM Basic is ready and available to perform administration tasks. It is ready to be used once the hardware is installed and connected to the Ethernet network.
- Familiar web browser-based graphical user interface that uses standard web browser applications for access. Online help is provided to aid users in performing tasks.

Key Terms

Here are key terms that will help you perform tasks such as zoning.

Fabric

Entity that interconnects N_Ports and is capable of routing (switching) Fibre Channel frames using the destination ID information in the Fibre Channel frame header accompanying the frames.

Storage Area Network (SAN)

A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated.

Zone (Zoning)

A group of devices or zone members in a SAN that can communicate and access each other. Communication is only allowed between devices in the same zone. A device can be in multiple zones so that shared resources can be accessed by many devices. Because SANs connect many types of devices that may carry different protocols, separating an entire fabric into zones can control access between specific devices. A zone (or zoning) is an efficient method of managing, partitioning, and controlling access to SAN devices. Zoning maximizes resources while maintaining data security and enabling heterogeneous systems and products to operate in the same SAN.

Zone Member

Specification (definition) of a device that belongs to a zone. A zone member can be identified by the port number of the device to which it is attached, by its device, by host bus adapter, or by world-wide name (WWN). In multiswitch fabrics, identification of end-devices and nodes by world wide name is preferable.

Zone Set

A set composed of one or more zones. When a zone set is activated, all zones in the set are activated at the same time. Only one zone set can be active in the fabric at one time and that zone set is referred to as the active zone set.

Suggested Reading

A book that can help you install products and configure a SAN is the *McDATA Products in a SAN Environment Planning Manual* (620-000124). You can obtain this book from the McDATA web site (www.mcdata.com) or from the documentation CD shipped with the McDATA product you purchased.

Another publication you may want to read is *An Introduction to Zoning*, which is a white paper on zoning fundamentals. It is available online from the McDATA web site at www.mcdata.com.

Where to Start

If the product has not been installed, you should start at Chapter 2, *Viewing Product Information*.

If the product was installed, then many of the configuration tasks were already completed. In that case, you may need to configure a zone. Configuring (including adding, deleting, and changing) zones is described in Chapter 4, *Configuring Zoning*

If the products have been configured and you have a functioning SAN, then you most likely will be interested in performing system administration tasks. Those tasks are described in Chapter 4, *Configuring Zoning*, Chapter 5, *Configuring Security*, and, Chapter 6, *Viewing System Logs*.

If you need to perform troubleshooting, then you will want to review Chapter 5, *Configuring Security*, and Chapter 6, *Viewing System Logs*.

Starting the EFCM Basic Interface

Open the EFCM Basic interface as follows:

1. You must be able to make a connection between the web browser and the product in order to log into the product. Ensure the workstation (or device you use to launch the web browser) and the Ethernet LAN segment containing the product, such as the 24-Port Switch, are attached and connected through the Internet.
2. Launch the web browser application (such as Netscape Navigator, version 7.0 or higher, or Microsoft Internet Explorer, version 6.0 or higher).
3. At the web browser, enter the IP address of the product as the Internet uniform resource locator (URL) such as *http://10.1.1.11*. For the ES-1000 Fabric Switch, the Enterprise Fabric Connectivity Manager (EFCM) and SANavigator SAN management tools provide a menu link that opens the web browser and connects to the EFCM Basic interface.

   NOTE: If the product has not been installed, refer to the product's installation and service manual for the default IP address, login ID, and password to use during installation.

4. After a connection is made between the web browser and the product, the *Enter Network Password* dialog box displays as shown in Figure 1-1. The dialog box may look different depending upon your system but in all cases, you need to enter a user name and password.

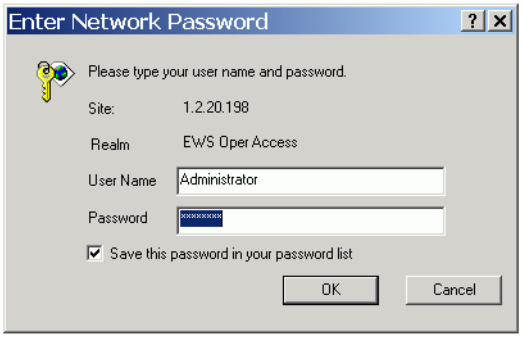


Figure 1-1 Enter Network Password Dialog Box

5. Type the user name and password. (The user name and password are case sensitive.)

   NOTE: The default user name is **Administrator** and the default password is **password.** After the initial log on, you will need to change the password for the user name, Administrator. During system installation, the default values may have been changed. If defaults have changed, contact your system administrator or the person who installed the product for the valid user names and passwords.

6. If you are logging onto EFCM Basic for the first time, the *First Time Login* page displays. Use this page to change the password for the default user name, Administrator. Enter the new password in the *New Password* and *Confirm Password* and then select *Activate* to save the new password.
7. Click *OK*. The EFCM Basic interface opens with the *Fabric View* page displayed as shown in Figure 1-2. For information about how to use this screen, and how to access the menu bar for a product in the SAN, see Chapter 8, *Using the Fabric View*.

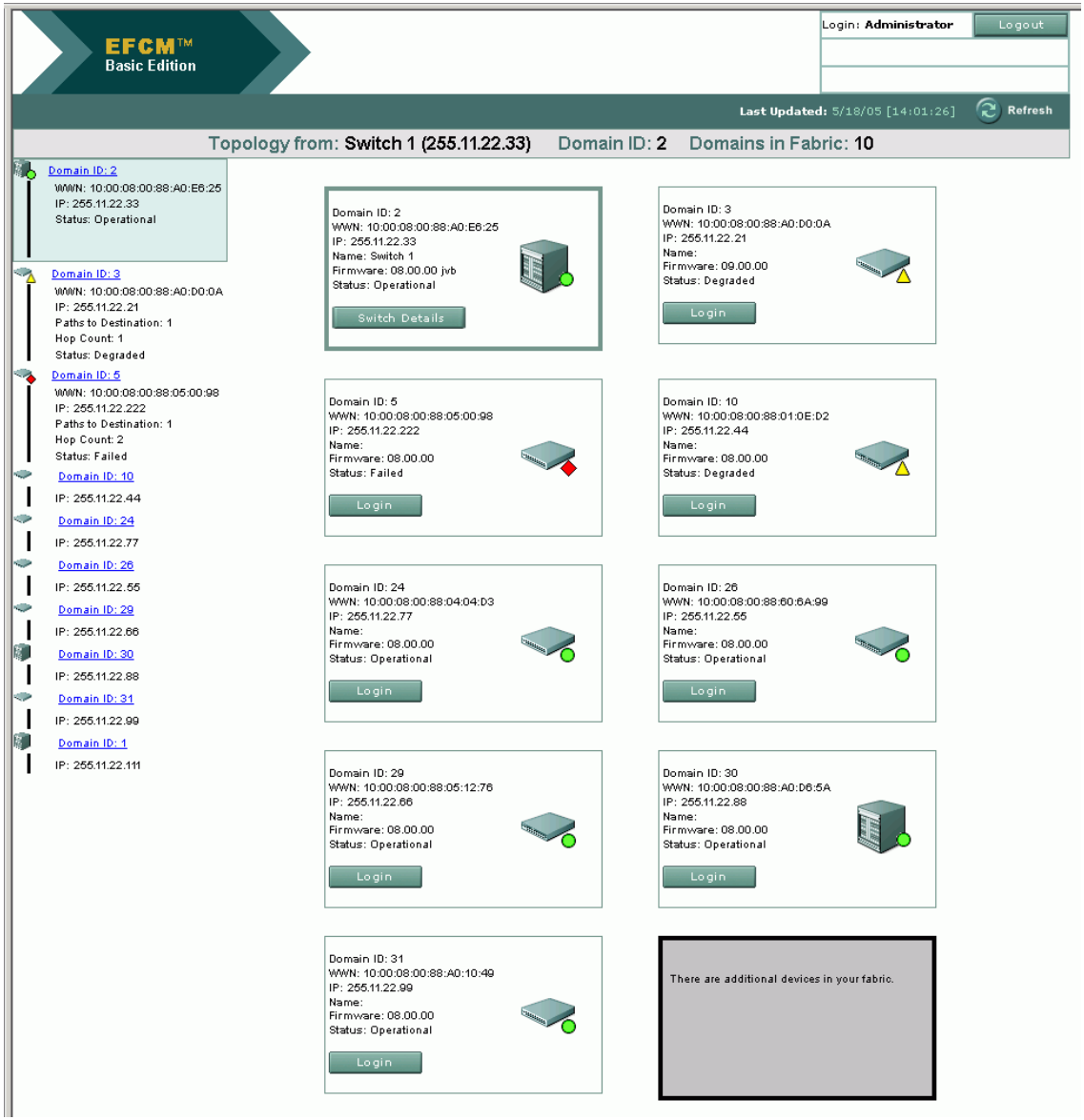


Figure 1-2 Fabric View

Using the EFCM Basic User Interface

When the EFCM Basic interface opens, the default display is the *Fabric View* screen. For information about how to use this screen, and how to access the menu bar for a product in the SAN, see Chapter 8, *Using the Fabric View*. To enable the full functionality of EFCM Basic for managing a product, you will need to select the *Switch Details* button for the product. This opens the Product Hardware page, and the menu bar and other functionality is enabled.

Figure 1-3 shows an example page from the interface. This example shows the *Product Hardware* screen for the 24-Port Switch. For other products, the corresponding page has a similar appearance.

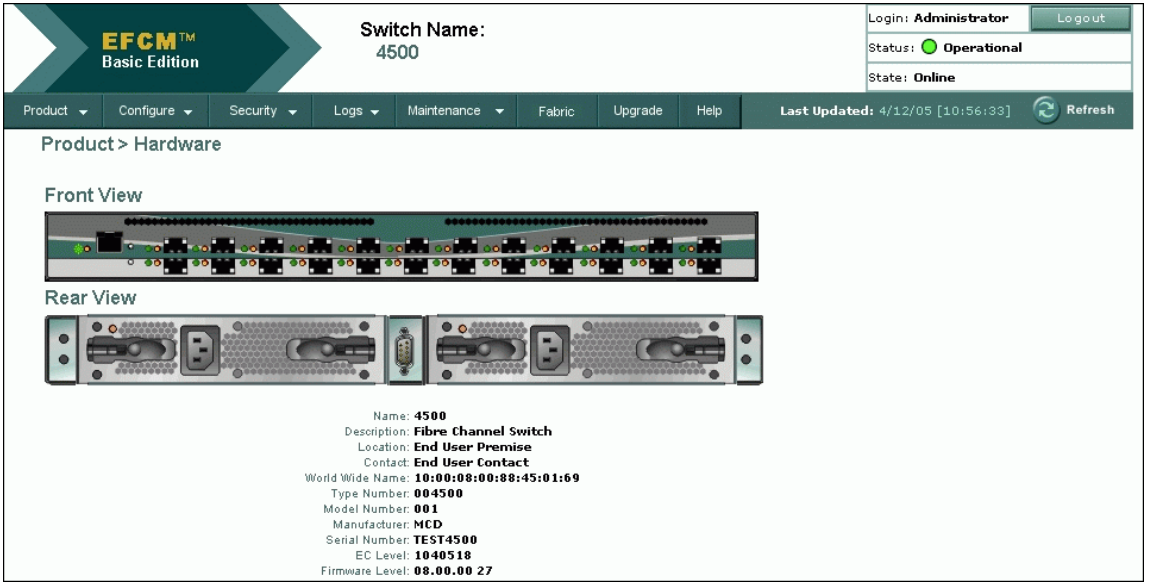


Figure 1-3 Example EFCM Basic Page Showing a 24-Port Switch

Navigational Tools of the EFCM Basic Page

The EFCM Basic interface has many buttons and other screen elements that appear in multiple views. These elements are broken out into the following categories:

- Tool bar options, which are described in Table 1-1 on page 1-11.
- Menu bar options, which are described in Table 1-2 on page 1-12.
- Page options, which are described in Table 1-3 on page 1-12.

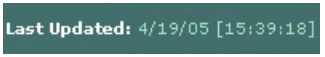
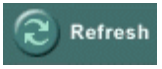
The tool bar displays the information described in the following table:

Table 1-1 Items on the Tool Bar

Item	Description
Switch Name	The user-defined name or description assigned to the product.
Logout button	Select this button to log out of EFCM Basic.
Login	The role of the user ID currently logged into the machine. This identifies whether the user has the rights of an Administrator or Operator. (Some functions and views are not available to the Operator level user.)
Status	The product's operational status: *Operational*, *Degraded*, or *Failed*.
State	The product's operational state. Valid values are: Offline — When the product is OFFLINE, all ports are offline. The ports cannot accept a login from an attached device and cannot connect to other switches. You can configure this state through the *Online State* page (*Set the Product Online State* on page 7-2). Online — All unblocked ports are able to connect with devices. You can configure this state through the *Online State* page (*Set the Product Online State* on page 7-2). Note that the product automatically goes online after a power-up, an initial machine load (IML), or initial program load (IPL).

The menu bar displays the information described in the following table:

Table 1-2 Items on the Menu Bar

Item	Associated Graphic	Description
Menus	N/A	Select a menu to display the menu items that are associated with the menu.
Help		Select the Help button to display procedures and descriptions for using EFCM Basic.
Last Updated Field		This field shows the last time the page was updated. For some pages, such as logs, this indicates the time when the information shown on the page was current. The status of the product or fabric may have changed after the last refresh of the page.
Refresh button		Select the Refresh button to update the page with current information.

The following items appear on multiple screens in the EFCM Basic interface:

Table 1-3 Items Used in Multiple Pages

Item	Associated Graphic	Description
Jump to Port field		This option is useful on products that have a large number of ports, so that only a fraction of the ports can be visible on the page at a time. Enter the port number of the port which you want to view and select the *Go* button.
Go button		After entering a port number in the *Jump to Port* field, select the *Go* button to view the port.
Links in the page		Text shown that is blue and underlined is a link. Click on the text to view the link information.
OK button		After making a change on a page, select the *OK* button to approve the change.

Table 1-3 Items Used in Multiple Pages (Continued)

Item	Associated Graphic	Description
Cancel button		After making a change on a page that is not already activated, select the *Cancel* button to cancel the change and redisplay the currently saved settings.
Arrow buttons		The arrow buttons are used to move items between panels in the page. Selecting an arrow moves the selected item in the direction the arrow is pointing.

Licensed Features

The EFCM Basic interface has many pages that require the purchase of licenses to activate their function. If you access a page that shows the text "Sample Only," using the page requires the installation of the license that enables the page's function.

For more information about upgrading your system with licensed features, see Chapter 9, *Software Upgrade and Feature Installation*.

2

Viewing Product Information

This chapter describes how to view configuration information of McDATA SAN products using the EFCM Basic interface. This chapter describes how to perform the following tasks:

- *Opening the Hardware Page* 2-1
- *Viewing the Port List* 2-4
- *Viewing the FRU List* 2-11
- *Viewing Operating Parameters* 2-12
- *Viewing the Node List* 2-14
- *Viewing Performance Information* 2-15

Opening the Hardware Page

The *Product* panel of the EFCM Basic interface enables you to see a representation of the physical product, whether a director or switch, and view the various IDs and configuration items for the product.

To view the representation of the product, select *Product* > *Hardware* from the navigation panel, or select the *Switch Details* button on the *Fabric View* page. The *Hardware* page displays. Figure 2-1 on page 2-2 shows an example of the *Hardware* page, showing a 24-port switch:

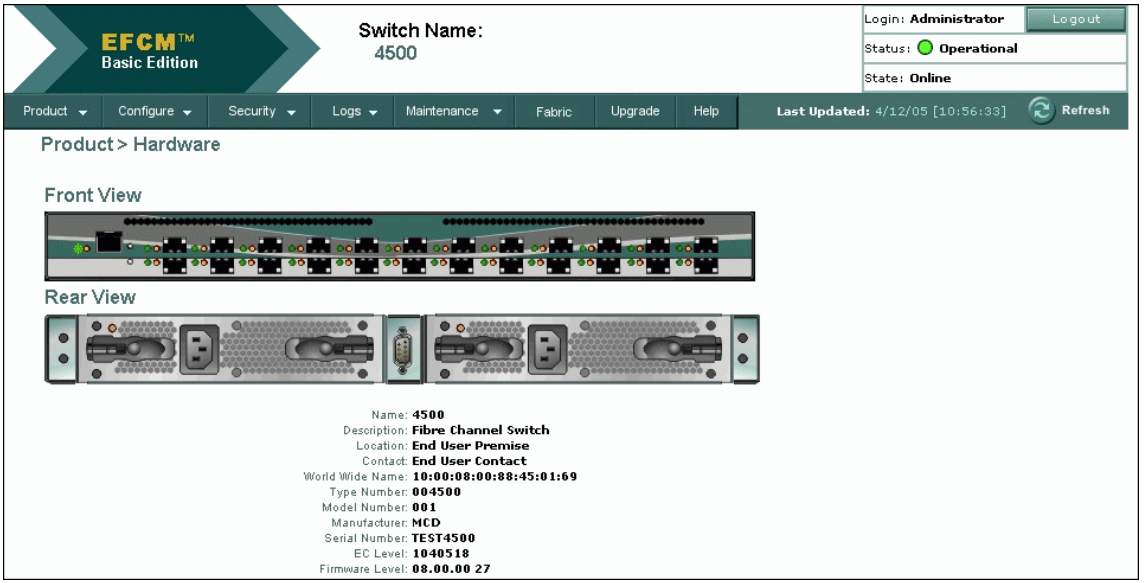


Figure 2-1 Product Hardware Page

Front View and Rear View

The *Hardware* page provides a representation of the front and rear views of the product. Using this graphical view of the product, you can view status symbols and simulated light emitting diode (LED) indicators, display data, or use mouse functions to monitor status and obtain vital product information for the product and its hardware components.

Move the cursor over parts of the graphics to display labels identifying each hardware component or port and its slot position in the chassis. Select a port to view the corresponding *Port List* information for the port (*Viewing the Port List* on page 2-4). Select a FRU to view the *FRU List* information for the FRU (*Viewing the FRU List* on page 2-11).

Colored indicators reflect the status of the actual LEDs on the product's components. Table 2-1 on page 2-3 describes the port operational states and the LED and attention indicators that display on the *Switch* or *Director* page.

NOTE: On the 140-Port Director, each of the installed port card FRUs bears a notation of either FPM, UPM or XPM to inform the user whether they are a 1 Gbps FPM, a 2 Gbps UPM, or a 10 Gbps XPM.

Table 2-1 Status Indicators

View	LED Name	Color	Behavior
Front	System Power	Green	• On when the LAN link is up.
	System Error Light (SEL)	Amber	• Off when the SEL on the hardware is off. • On when the SEL on the hardware is on. When this indicator illuminates, an event has occurred requiring immediate attention, such as a system, fan, power supply, or port failure.
	Port Online	Green/Blue	• Off when port status is anything but Online. • On when port status is Online and the operating speed is 1 Gbps, 2 Gpbs, 4 Gbps, or 10 Gbps.
	Port Service Required	Amber	• Off when port status is anything but Failed or Service Required. • On when port status is Failed or Service Required.
Rear	FRU Service Required	Amber	• Off when FRU status is Active. • On when FRU status is Failed.

Product Information

Below the illustration of the front and rear views of the product, the following information displays:

- **Name**—The name configured for the product.
- **Description**—A configurable description of the product functionality.
- **Location**—Location of the product.
- **Contact**—Name of the product's point of contact.
- **World Wide Name**—Fibre Channel WWN address.

- **Type Number**—Type number of the product, usually the numeric part of the product's name.
- **Model Number**—Model number of the product.
- **Manufacturer**—Three-letter identifier of the product's manufacturer.
- **Serial Number**—Product serial number.
- **EC Level**—Current engineering change (EC) level.
- **Firmware Level**—Release number of the firmware that is installed.

Viewing the Port List

Select *Product* > *Port List* on the navigation panel. The *Port List* page displays (Figure 2-2 on page 2-5). This page has two parts:

- Port List—The upper part of the page shows a list of ports and information about the ports. If you select the links on the list of ports, information on the lower part of the page is updated for that port. For more information about this page, see *Port List* on page 2-5.
- Detailed Information—The lower part of the page shows detailed information about items selected on the Port Table. You can view the following types of information:
  - *Port Information* on page 2-7
  - *Health Status Information* on page 2-9
  - *Transceiver Information* on page 2-10

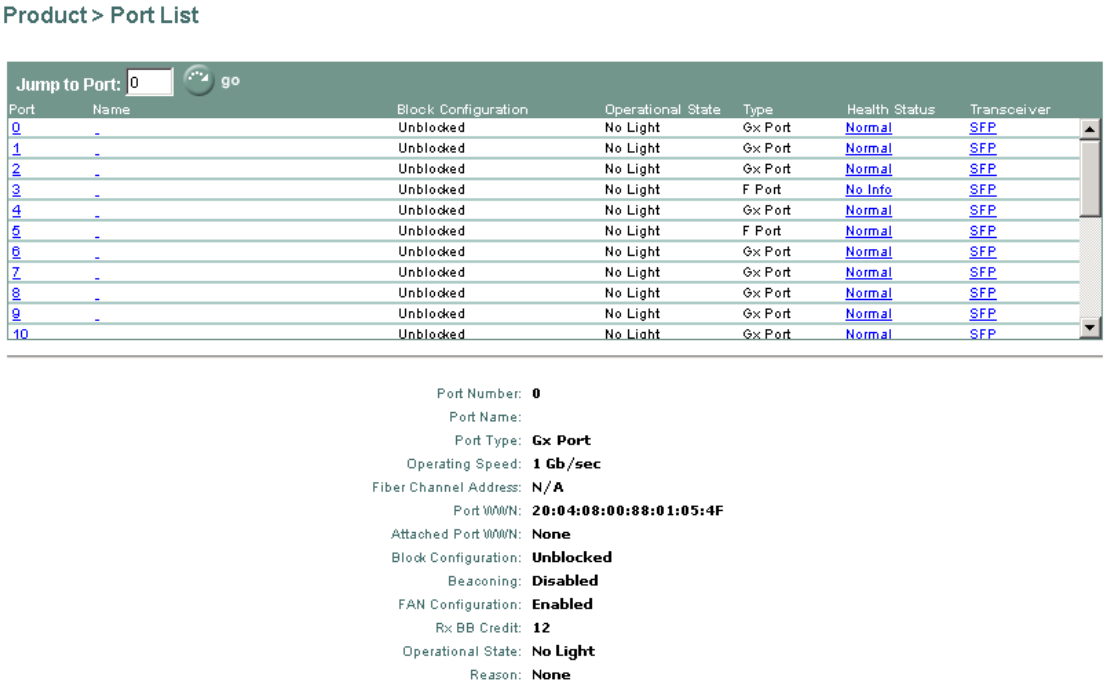

Product > Port List
Jump to Port: 0 go
Port Name Block Configuration Operational State Type Health Status Transceiver
0 Unblocked No Light Gx Port Normal SFP
1 Unblocked No Light Gx Port Normal SFP
2 Unblocked No Light Gx Port Normal SFP
3 Unblocked No Light F Port No Info SFP
4 Unblocked No Light Gx Port Normal SFP
5 Unblocked No Light F Port Normal SFP
6 Unblocked No Light Gx Port Normal SFP
7 Unblocked No Light Gx Port Normal SFP
8 Unblocked No Light Gx Port Normal SFP
9 Unblocked No Light Gx Port Normal SFP
10 Unblocked No Light Gx Port Normal SFP
Port Number: 0
Port Name:
Port Type: Gx Port
Operating Speed: 1 Gb/sec
Fiber Channel Address: N/A
Port WWN: 20:04:08:00:88:01:05:4F
Attached Port WWN: None
Block Configuration: Unblocked
Beaconing: Disabled
FAN Configuration: Enabled
Rx BB Credit: 12
Operational State: No Light
Reason: None

Figure 2-2 Port List Page

Port List

The scroll list part of the *Port List* page provides the following information for all of the ports on the product:

- **Port #**—The number of the port.
- **Name**—Displays the port name as configured. For instructions for setting the port name, see *Configuring Basic Port Information* on page 3-2.
- **Block Configuration**—Indicates the blocked or unblocked configuration of the port:
  - — Blocked: Devices communicating with the port are prevented from logging into the product or communicating with other devices attached to product ports.
  - — Unblocked: Devices communicating with the port can log into the product and communicate with devices attached to any other unblocked port in the same zone.

- **Operational State**—refer to *Port Operational States* on page 2-6 for an explanation of the states.
- **Type**—The type of port. The valid options vary by product. (This may be the same as the configured port type.)
- **Health Status**—Status of the installed optic for the port. Values for this parameter are *Normal*, *Warning*, *Alarm*, and *No Info*.
- **Transceiver**—The transceiver type of the installed optic.

Port Operational States

The *Operational State* column of the *Port List* page displays one of the following operational states:

- **Beaconing**—The port is beaconing, which means that the beaconing light is flashing on the physical hardware. (A port in a failed state cannot beacon.)
- **Inactive**—The switch port is in an inactive state. Reasons for this state appear in the *Reason* field in the lower part of the page when the port is selected. (Refer to *Port Information* on page 2-7 for more information.)

TIP: Note that if port optics have also failed, the amber LED will be on.

- **Invalid Attachment**—The switch port is in an invalid attachment state.
- **Link Incident**—A link incident occurred on one of the ports.
- **Link Reset**—The switch and the attached device are performing a link reset operation to recover the link connection. Ordinarily, this is a transient state.
- **No Light**—No signal (light) is being received on the switch port. This is a normal condition when there is no cable plugged into the port or when the power of the device attached to the other end of the link is off.
- **Not installed**—The port optics are not installed or the feature that provides additional port function is not enabled.
- **Not Operational**—The switch port is receiving the Fibre Channel not operational sequence (NOS) indicating that the attached device is not operational.
- **Online**—The attached device has successfully connected to the switch and is ready to communicate, or is in the process of communicating with other attached devices.

- **Offline**—The switch port was configured as "blocked" and is transmitting the Fibre Channel OLS to the attached device.
- **Port Failure**—The switch port has failed and requires service. (A port in the failed state cannot beacon.)
- **Segmented**—The E_Port is segmented preventing the two fabrics from joining (this only occurs when two switches are connected to each other).
- **Testing**—Port is executing an internal loopback test.

Port Information

If you select a port number or port name, the lower part of the *Port List* page (Figure 2-2 on page 2-5) provides the following information for the selected port:

- **Port Number**—The physical port number.
- **Port Name**—User-defined port name or description.
- **Type**—The configured port type. Valid options vary by product, but the valid options are:
  - — G_Port. This displays if nothing is logged into the port and the port is configured to be a G_Port.
  - — F_Port. This displays if a device is logged into the port.
  - — E_Port. This displays if the port is connected to another switch's E_Port through an ISL.
  - — GX_Port. Valid only on loop devices, allows a port to operate as either a Fabric Loop Port, Fabric Port, or an Expansion Port. This displays if nothing is logged into the port and the port is configured to be a GX_Port.
  - — FX_Port. Valid only on loop devices. This setting restricts a port to operate as either a Fabric Loop Port or a Fabric Port.
- **Operating Speed**—This field displays the current data speed for the port as *1 Gb/sec*, *2 Gb/sec*, or *Not Established*. *Not Established* displays if *Negotiate* is defined as the operating speed and the data speed has not been resolved between the port and the attached device, or if the port and device are not communicating. Note that *2 Gb/sec* and *Not Established* can display only on machines that support 2 Gbps speeds.
- **Fibre Channel Address**—Fibre Channel Address identifier of the port. Not displayed for some products.

- **Port WWN**—The port's 16-digit WWN.
- **Attached Port WWN**—Fibre Channel WWN identifier of the device attached to the port. (This field is not valid for loop devices.)
- **Block Configuration**—Indicates whether the port is blocked or unblocked.
- **Beaconing**—This field indicates the beaconing status for the port.
- **FAN Configuration**—This field indicates the FAN status for the port. This field is valid only on the products that support arbitrated loop devices.
- **Rx BB Credit**—The number of receive buffer-to-buffer credits (BB_Credits) configured for the port.
- **Operational State**—Inactive, invalid attachment, link incident, no light, not operational, online, offline, port failure, segmented E_Port, testing, or not installed.
- **Reason**—When the port operating state is *Segmented*, *Invalid Attachment*, or *Inactive*, this field displays the reason for that state. When an E_Port is segmented, two fabrics are prevented from joining. This only occurs when the switch is attempting to connect to another switch. Reasons and probable causes are listed under reason field messages below.

  — If Operational State is *Segmented*:

    - Segment Not Defined
    - Incompatible Operating Parameters
    - Duplicate Domain IDs
    - Incompatible Zoning Configurations
    - Build Fabric Protocol Error
    - No Principal Switch
    - No Response from Attached Switch
    - ELP Retransmission Failure Timeout
    - Link Parameter mismatch

  — If Operational State is *Invalid Attachment*:

    - Unknown

- ISL connection not allowed on this port
- ELP rejected by the attached switch
- Incompatible switch at other end of the ISL
- External loopback adapter connected to the port
- N_Port connection not allowed on this port
- Incompatible non-McDATA switch at other end of the ISL
- ISL connection not allowed to external Fabrics
- Port binding violation - unauthorized WWN
- Unresponsive node connected to Port

— If Operational State is *Inactive*:

- No Serial Number
- No Key Enabled
- Switch Speed Conflict
- Optics Speed Conflict (64-Port and 140-Port Directors only)
- No SBAR Support (64-Port and 140-port Directors only)

Health Status Information

If you select the entry for a port in the *Health Status* column, Predictive Optics Monitoring (POM) information displays. POM data for the selected port appears in the lower part of the page:

- **Port Number**—Product port number.
- **Health Status**—Condition of the installed optical transceiver (*Normal*, *Warning*, *Alarm*, or *No Info*).
- **Transceiver Type**—Installed transceiver type (*SFP*, *XFP*, or *Unknown*).

If the port has a digital diagnostics (DD) enabled optical transceiver installed, product firmware displays a table of reported temperature, voltage, current, transceiver power, and receiver power (Figure 2-3 on page 2-10). Optical transceivers also provide vendor-specific threshold values for these parameters.

Port Number: **0** Health Status: **Normal** Transceiver Type: **SFP**

	Temperature [C]	Supply Voltage [V] 3.3	Bias Current [mA]	TX Power [uW]	RX Power [uW]
Measured Result	28.203	3.282	6.320	315.000	218.400
Thresholds					
Alarm Max	95.000	3.630	28.000	794.300	1000.000
Warning Max	90.000	3.560	14.800	630.900	794.300
Warning Min	-25.000	3.040	4.600	141.300	31.600
Alarm Min	-30.000	2.970	3.100	125.900	25.100

Figure 2-3 Optics Monitoring Information

Transceiver Information

At the *Port List Page*, click the entry for a port in the *Transceiver* column. Port transceiver technology information for the selected port appears in the lower panel of the page:

- **Port Number**—Product port number.
- **Identifier**—Installed transceiver type (*SFP*, *XFP*, or *Unknown*).
- **Connection type**—Type of port connector (*LC*, *MT_RJ*, *MU*, *Unknown*, or *Internal Port*).
- **Transceiver**—Type of port transceiver (*Shortwave Laser*, *Longwave Laser*, *Long Distance Laser*, *Unknown*, or *None*).
- **Distance Capability**—Port transmission distance (*Short*, *Intermediate*, *Long*, *Very Long*, or *Unknown*).
- **Media**—Type of optical cable used (*Singlemode*, *multimode 50-micron*, *multimode 62.5-micron*, or *Unknown*).
- **Speed**—Operating speed (*Unknown*, *1 Gbps*, *2 Gbps*, *4 Gbps*, or *10 Gbps*).

Viewing the FRU List

Select *Product* > *FRU List* on the navigation panel. The *FRU List* page (Figure 2-4) displays.

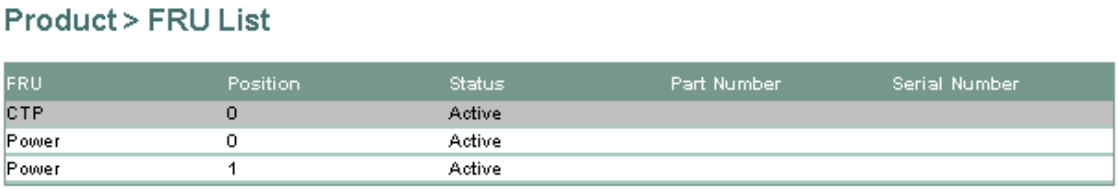


Figure 2-4 FRU List Page

This page shows the following information for the FRUs:

- **FRU**—Name of the FRU.
- **Position**—Slot position relative to identical FRUs installed in the chassis.
- **Status**—Status of the FRU: Active, Backup, Failed or Not Installed.
- **Part number**—The OEM part number, as set in non-volatile memory of the FRU (if applicable).
- **Serial number**—Serial number of the FRU, as set in its non-volatile memory (if applicable).

Viewing Operating Parameters

To view the Operating Parameters of a product, perform the following procedure:

1. From the navigation panel, select *Product* > *Operating Parameters*. The *Operating Parameters* page displays (Figure 2-5) showing *Switch Parameters* and *Fabric Parameters*.

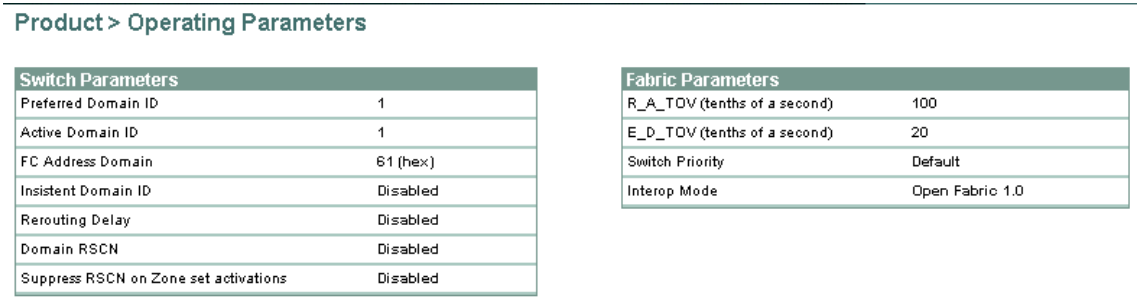

Product > Operating Parameters
Switch Parameters
Preferred Domain ID 1
Active Domain ID 1
FC Address Domain 61 (hex)
Insistent Domain ID Disabled
Rerouting Delay Disabled
Domain RSCN Disabled
Suppress RSCN on Zone set activations Disabled
Fabric Parameters
R_A_TOV (tenths of a second) 100
E_D_TOV (tenths of a second) 20
Switch Priority Default
Interop Mode Open Fabric 1.0

Figure 2-5 Operating Parameters Page

Switch Parameters

This page shows the following *Switch Parameters* information for the product:

- **Preferred Domain ID**—The ID to be used if the product participates in a multi-switch fabric. The preferred domain ID must be unique for each director and switch in a fabric.
- **Active Domain ID**—The domain ID assigned to the switch.
- **FC Address Domain**—The value of the domain byte of the Fibre Channel Address for ports on this product.
- **Insistent Domain ID**—Indicates whether the domain ID is enabled to be insistent. This option is required if Enterprise Fabric Mode (an optional SANtegrity Binding feature) or Fabric Binding is enabled.
- **Rerouting Delay**—Indicates whether rerouting delay is enabled. Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination.

- **Domain RSCN**—If enabled, domain registered state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to HBAs and storage devices. This option is required if Enterprise Fabric Mode (an optional SANtegrity Binding feature) is enabled.
- **Suppress RSCN on Zone Set Activations**—If enabled, registered state change notification (RSCN) messages are prohibited from being sent to ports on the switch following any change to the fabric's active zone set. If the state shown is disabled, RSCN messages are sent to ports on the switch for changes to the fabric's active zone set.
- **Director Speed**—Speed of communications on the product. Values can be *1 Gbps* or *2 Gbps*. Valid on the 64-Port Director only.

Fabric Parameters

This page shows the following *Fabric Parameters* information for the product:

- **R_A_TOV**—Resource Allocation Time Out Value (R_A_TOV) used by the fabric. Specified in tenths of a second.
- **E_D_TOV**—Error Detection Time Out Value (E_D_TOV) value used by the fabric. Specified in tenths of a second.
- **Switch Priority**—Priority value of the switch. Values can be *Default*, *Principal*, and *Never Principal*.
- **Interop Mode**—Interoperability mode of the fabric. Values can be *McDATA Fabric 1.0* and *Open Fabric 1.0*. (This field is not valid if the product's Operation Mode is *S/390*[1].)

1. The Operation Mode parameter of the EFCM Basic interface is equivalent to the Management Style parameter of the Element Manager interface. The S/390 Mode used for the EFCM Basic interface is equivalent to the FICON management style on the Element Manager.

Viewing the Node List

Select *Product* > *Node List* on the navigation panel. The *Node List* page (Figure 2-6) displays.

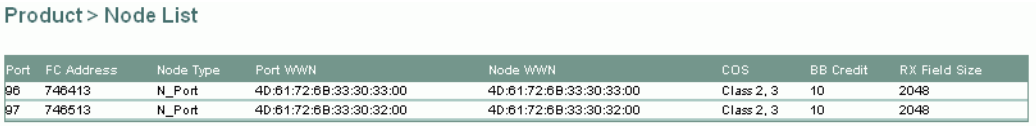

Product > Node List
Port FC Address Node Type Port WWN Node WWN COS BB Credit RX Field Size
96 746413 N_Port 4D:61:72:6B:33:30:33:00 4D:61:72:6B:33:30:33:00 Class 2, 3 10 2048
97 746513 N_Port 4D:61:72:6B:33:30:32:00 4D:61:72:6B:33:30:32:00 Class 2, 3 10 2048

Figure 2-6 Node List Page

Information displayed for each node includes:

- **Port**—The number of the port.
- **FC Address**—Fibre Channel Address identifier of the port. Not displayed for some products.
- **Node Type**—Type of node.
- **Port WWN**—The WWN assigned to the port.
- **Node WWN**—The node's WWN.
- **COS (Class of Service)**—Class 2 and/or Class 3 service.
- **BB_Credit**—The BB_Credits the attached node has available.
- **RX Field Size**—The largest Fibre Channel frame the node can process.

Viewing Performance Information

Select *Product* > *Performance* on the navigation panel. The *Performance* page (Figure 2-7 on page 2-16) displays. The Performance page provides port utilization percentages and error totals for all ports and the following types of information for the selected port:

- *Traffic Statistics* on page 2-16
- *Error Statistics* on page 2-17
- *Class 2 Statistics* on page 2-19
- *Class 3 Statistics* on page 2-19
- *Open Trunking Statistics* on page 2-19

To select a port, click on the port's number or name, shown in the *Port* and *Name* fields.

Using the Performance Page

The *Performance* page provides the following functions:

- **Jump to Port**—Use this field to specify a port to display in the page. Click the *Go* button to view the port.
- **Clear All**—Select this button to reset all statistics for all ports to zero.

NOTE: Cleared fields may not show a value of 0 when they are cleared, if data traffic is flowing through the port.

- **Clear**—Select this button to set statistics for the selected port to zero. Values for other ports are not affected.

Parts of Statistics Tables

The tables of statistics contain the following columns:

- **Statistics**—The type of statistic being tracked.
- **# of Wraps**—Number of times the *Counter* value wraps, for statistics that grow rapidly. The maximum value that either the *Counter* or the *# of Wraps* can hold is 2^{32}, or 4,294,967,296. Each time the *Counter* field reaches the maximum value of 2^{32}, the wrap count is incremented by 1.
- **Counter**—The number of instances of the tracked item recorded since system initialization or the last time the counters were cleared.

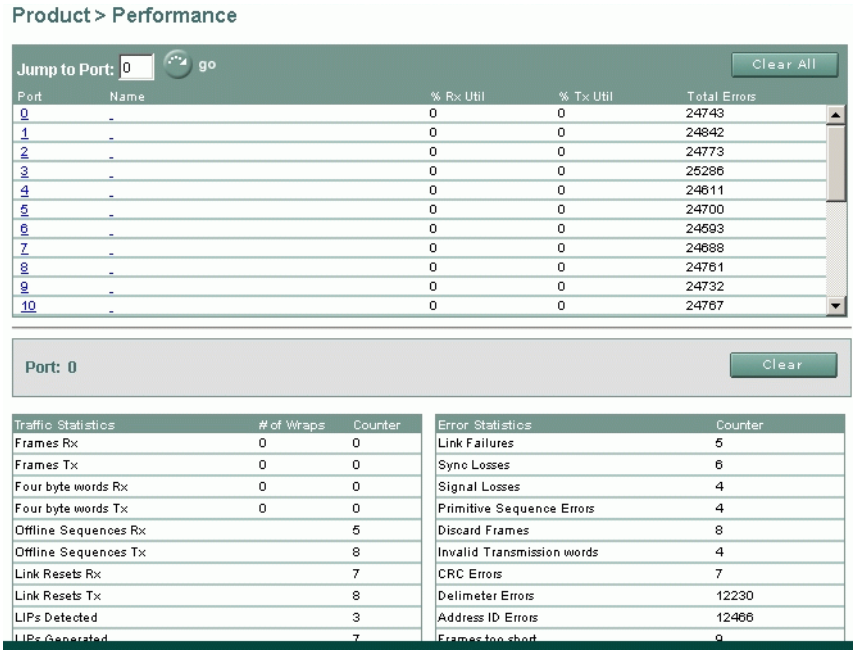

Product > Performance
Jump to Port: 0 go
Clear All
Port Name % Rx Util % Tx Util Total Errors
0 - 0 0 24743
1 - 0 0 24842
2 - 0 0 24773
3 - 0 0 25286
4 - 0 0 24611
5 - 0 0 24700
6 - 0 0 24593
7 - 0 0 24688
8 - 0 0 24761
9 - 0 0 24732
10 - 0 0 24767
Port: 0
Clear
Traffic Statistics # of Wraps Counter
Frames Rx 0 0
Frames Tx 0 0
Four byte words Rx 0 0
Four byte words Tx 0 0
Offline Sequences Rx 5
Offline Sequences Tx 8
Link Resets Rx 7
Link Resets Tx 8
LIPs Detected 3
Error Statistics Counter
Link Failures 5
Sync Losses 6
Signal Losses 4
Primitive Sequence Errors 4
Discard Frames 8
Invalid Transmission words 4
CRC Errors 7
Delimeter Errors 12230
Address ID Errors 12466

Figure 2-7 Product Performance Page

Port Utilization Percentages and Error Totals

The *Performance* page provides utilization information and error totals for each port as described below:

- **Port**—The port number.
- **Name**—The configured port name.
- **% Rx Util**—Percentage of received link traffic on the port that is data.
- **% Tx Util**—Percentage of transmitted link traffic on the port that is data.
- **Total Errors**—The total number of errors received on the port.

Traffic Statistics

The *Performance* page provides the following traffic statistics for the selected port:

- **Frames Rx**—The number of frames that the port has received.
- **Frames Tx**—The number of frames that the port has transmitted.

- **Four byte words Rx**—The number of words that the port has received.
- **Four byte words Tx**—The number of words that the port has transmitted.
- **Offline sequences Rx**—The number of offline sequences (OLS) received by this port.
- **Offline sequences Tx**—The number of offline sequences (OLS) transmitted by this port.
- **Link resets Rx**—The number of link reset protocol frames received by this port from the attached N_Port.
- **Link resets Tx**—The number of link reset protocol frames transmitted by this port to the attached N_Port.
- **Link utilization % Rx**—The current receive link utilization for the port expressed as a percentage. On 1 Gbps links, ports can transmit or receive data at 100 MB per second. On 2 Gbps links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.
- **Link utilization % Tx**—The current transmit link utilization for the port expressed as a percentage. On 1 Gbps links, ports can transmit or receive data at 100 MB per second. On 2 Gbps links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.
- **Time Spent at 0 Tx BB Credit**—The amount of time that the port has had no transmit BB_Credits available.

For the loop devices, the following statistics are also shown:

- **LIPs Detected**—A loop initialization primitive was detected, which means the loop was completed.
- **LIPs Generated**—A loop initialization primitive was created to initialize a loop.

Error Statistics

The *Performance* page provides the following error statistics for the selected port:

- **Link failures**—The number of link failures recorded because a not operational sequence (NOS), protocol timeout, or port failure was detected.

- **Sync losses**—The number of loss-of-synchronizations detected because an attached device was reset or disconnected from the port.
- **Signal losses**—The number of loss-of-signal errors detected because the attached device was reset or disconnected from the port.
- **Primitive sequence errors**—The number of primitive sequence protocol errors received from an attached device, which indicates a Fibre Channel link-level protocol violation.
- **Discard frames**—A received frame could not be routed and was discarded because the frame timed out due to an insufficient buffer-to-buffer credit, or the destination device was not logged into the product.
- **Invalid transmission words**—The number of invalid transmission words from an attached device. This indicates that a frame or primitive sequence arrived at the port corrupted.
- **CRC errors**—A received frame failed a cyclic redundancy check (CRC) validation, indicating the frame arrived at the port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure, a bad fiber-optic cable, or a poor cable connection.
- **Delimiter errors**—The number of times that the switch detected an unrecognized start-of-frame (SOF), an unrecognized end-of-frame (EOF) delimiter, or an invalid class of service. This indicates that the frame arrived at the switch's port corrupted. This corruption can be due to plugging/unplugging the link, bad optics at either end of the cable, bad cable, or dirty or poor connections. Moving the connection around or replacing cables can isolate the problem.
- **Address ID errors**—A received frame had an unavailable or invalid Fibre Channel destination address, or an invalid Fibre Channel source address. This typically indicates the destination device is unavailable.
- **Frames too short**—A received frame exceeded the Fibre Channel frame maximum size or was less than the Fibre Channel minimum size, indicating the frame arrived at the switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

Class 2 Statistics

The *Performance* page provides the following Class 2 statistics for the selected port:

- **Received Frames**—The number of Class 2 frames received by this F_Port from its attached N_Port.
- **Transmitted Frames**—The number of Class 2 frames transmitted by this F_Port to its attached N_Port.
- **4-byte words Rx**—The number of Class 2, 4-byte words received by the port.
- **4-byte words Tx**—The number of Class 2, 4-byte words transmitted by the port.
- **Busied Frames**—The number of F_BSY frames generated by this F_Port against Class 2 frames.
- **Rejected Frames**—The number of F_RJT frames generated by this F_Port against Class 2 frames.

Class 3 Statistics

The *Performance* page provides the following Class 3 statistics for the selected port:

- **Received Frames**—The number of Class 3 frames received by the F_Port from its attached N_Port.
- **Transmitted Frames**—The number of Class 3 frames transmitted by this F_Port to its attached N_Port.
- **Discarded Frames**—The number of Class 3 frames discarded (including multicast frames with bad domain IDs).
- **4-byte words Rx**—The number of Class 3, 4-byte words received by the port.
- **4-byte words Tx**—The number of Class 3, 4-byte words transmitted by the port.

Open Trunking Statistics

The *Performance* page provides the following Open Trunking statistics for the selected port:

- **Flows rerouted to ISL**—The number of Fibre Channel traffic flows that were rerouted to this ISL from another ISL due to congestion. (This value increments only if the OpenTrunking feature is installed.)

- **Flows rerouted from ISL**—The number of Fibre Channel traffic flows that were rerouted from this ISL to another ISL due to congestion. (This value increments only if the OpenTrunking feature is installed.)

3

Configuring the Product

This chapter describes how to configure products using the EFCM Basic interface. These procedures can be used to configure a product after installation and as changes are needed.

You can use the options on the *Configure* menu to perform configuration tasks for your product:

- *Factory Default Values* 3-2
- *Configuring Ports* 3-2
  - — *Configuring Basic Port Information* 3-2
  - — *Configuring Port Rx BB_Credits* 3-5
  - — *Configuring NPIV* 3-7
- *Configuring Switch Information* 3-9
  - — *Configuring Switch Identification* 3-9
  - — *Configuring Switch Date and Time* 3-10
  - — *Configuring Switch Parameters* 3-11
  - — *Configuring Fabric Parameters for the Switch* 3-14
  - — *Configuring Network Parameters for the Switch* 3-16
- *Configuring SNMP* 3-18
- *Configuring CLI and SSH* 3-19
- *Configuring OSMS and Host Control* 3-20
- *Configuring SSL* 3-21
- *Zoning* 3-24
- *Configuring Performance Parameters* 3-25
  - — *Configuring Open Trunking* 3-25
  - — *Configuring Preferred Paths* 3-27
- *Configuring Port Fencing* 3-30
- *Setting a Switch Online and Offline* 3-32
- *Enabling and Disabling Software* 3-33
- *Enabling and Disabling the CLI* 3-33
- *Upgrade Options* 3-34

Factory Default Values

McDATA products on a SAN have pre-set, default configuration values that were set in the factory. The items that have factory-set default values are:

- Passwords (customer and maintenance-level)
- Internet Protocol (IP) address
- Subnet mask
- Gateway address

The specific default values associated with a particular product are documented in the installation and service manual for the product.

Configuring Ports

To configure ports, there are three pages:

- Basic Information—Enables you to configure basic aspects of a port. The port's name, blocked status, Fabric Address Notification (FAN) status, type and speed of a port.
- Rx BB Credit—Enables you to configure receive BB_Credits for a port.
- NPIV—Enables you to configure and enable NPIV functionality for a port.

Configuring Basic Port Information

The *Basic Information* page enables you to configure basic aspects of a port. The port's name, blocked status, FAN status, type, and speed are configured using this page.

NOTE: If you are going to change the *Speed* parameter on a 64-Port Director, set the product offline. To set the product offline, clear the *Switch Online* check box on the *Configure* menu.

Use the following procedure to set configure basic port information:

1. Select *Configure* > *Ports* > *Basic Information* on the navigation panel. The *Port Basic Information* page (Figure 3-1 on page 3-3) displays.

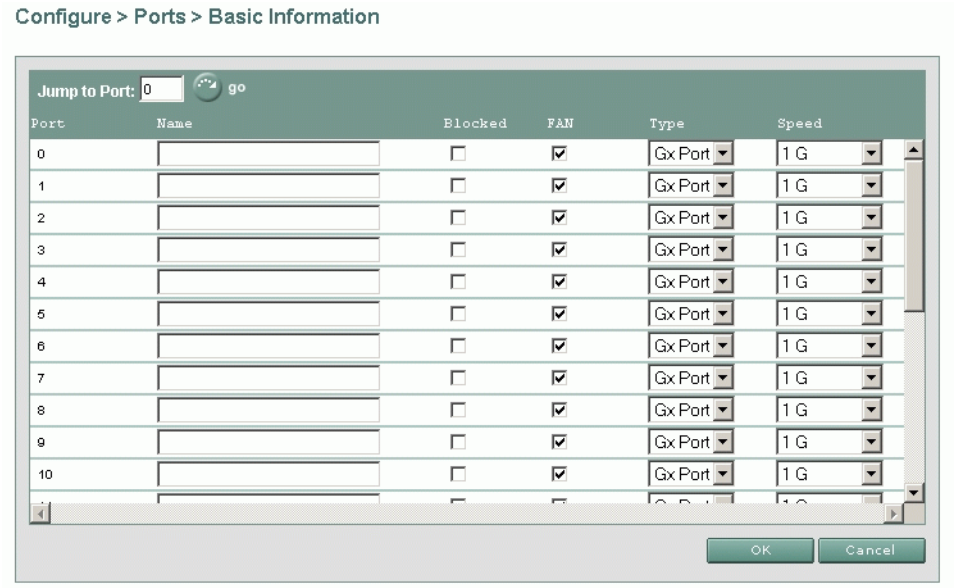


Figure 3-1 Port Basic Information Page

2. For each port to be configured, type a port name of 24 or fewer alphanumeric characters in the associated *Name* field.

TIP: When naming ports, you may want to name each port based on the device attached to the port. For example, if the port is attached to an e-mail server, you might name the port *email1 server port 2*. Relate the name of the port to the device that is attached to the port.

3. Click a check box in the *Blocked* column to block or unblock a port (default is unblocked). A check mark in the box indicates a port is blocked. Blocking a port prevents the attached devices or McDATA products in the fabric from communicating. A blocked port continuously transmits the offline sequence (OLS).

4. Click the check box in the *FAN* column to enable or disable the fabric address notification (FAN) feature (default is enabled). (The FAN column is available only on products that support arbitrated loop devices.) A check mark in the box indicates FAN is enabled. When the feature is enabled, the port transmits a FAN frame after loop initialization to verify that Fibre Channel Arbitrated Loop (FC-AL) devices are still logged in. It is recommended this option be enabled for ports configured for loop operation.

5. Select from the drop-down list in the *Type* column to configure the port type. Available selections are:
   - **G_Port**—Generic port.
   - **F_Port**—Fabric port.
   - **E_Port**—Expansion port.
   - **GX_Port**—Generic mixed port. Use this selection to configure a port as a generic loop port (GL_Port). The port automatically negotiates any connection type (loop devices only).
   - **FX_Port**—Fabric mixed port. Use this selection to configure a port as a fabric loop port (FL_Port). The port automatically negotiates only F_Port and FL_Port connections, which are available on loop devices only.

NOTE: On the 12-Port Switch, the E_Port, G_Port, and GX_Port options are not valid, unless the Fabric Capable feature is enabled. For more information, see the *McDATA Sphereon 4300 Switch Installation and Service Manual* (620-000171).

6. Select from the drop-down list in the *Speed* column to configure the port transmission rate. The drop-down list only contains the configured speeds for each individual port. For example, on a 10 Gb port, the drop-down list only displays one choice, 10 Gb/sec.
   - **Negotiate**—Auto-negotiate between 1.0625 and 2.125 gigabits per second (Gbps) operation. This is valid only on products that are capable of 2 Gbps operation.
   - **1 Gb/sec**—1.0625 Gbps operation.
   - **2 Gb/sec**—2.125 Gbps operation.
   - **4 Gb/sec**—4.25 Gbps operation.
   - **10 Gb/sec**—10.0 Gbps operation.

NOTE: The *Speed* parameter is not valid for all products.

7. Click *OK* to save and activate the changes. The message **Your changes to the port configuration have been successfully activated** appears.
8. If the product is offline, set the product online by selecting the *Switch Online* check box on the *Configure* menu.

Configuring Port Rx BB_Credits

Use the *Rx BB Credit* page to configure the BB_Credit allocation for ports on the product. For each type of port, there is a maximum and minimum BB_Credit limit which is displayed as a range. For a detailed explanation of BB_Credits, see the *McDATA Products in a SAN Environment Planning Manual* (620-000124).

The *Rx BB Credit* page contains a list of ports and their corresponding BB_Credits value and other values. For some products, the page also contains a *Buffer Pool Status* section. Some products have a predefined pool of BB_Credits, which is shared by all of the product's ports. This pool is defined by the maximum number of BB_Credits that can be assigned on the product. You cannot assign more BB_Credits than the number of BB_Credits in the pool. The *Buffer Pool Status* section provides the following information:

- Maximum Buffer—The maximum number of BB_Credits in the buffer pool. This value is determined by the type of product.
- Allocated Buffers—The number of BB_Credits in the buffer pool that have already been assigned to all ports on the product.
- Unallocated Buffers—The number of BB_Credits in the buffer pool that have not been assigned to any ports and are available for assignment.

For information about how BB_Credits are assigned on your product, see the product's *Installation and Service Manual*.

Use the following procedure to configure BB_Credits values for ports:

1. If you are setting BB_Credit values for all ports, set the product offline. To set the product offline, clear the *Switch Online* check box on the *Configure* menu.

   If you are configuring individual ports, set them offline by blocking them, as described in *Configuring Basic Port Information* on page 3-2.

   NOTE: If a port is online, you are not able to change its BB_Credit value; the *RX BB Credit* field is not enabled.

2. Select *Configure* > *Ports* > *Rx BB Credit* on the navigation panel. The *Rx BB Credit* page (Figure 3-2 on page 3-6) displays.

Figure 3-2 Rx BB_Credit Page

3. Verify that the port is offline by checking the value in the *State* column.
4. Each port has a maximum and minimum number of BB_Credits that can be assigned to it, based on the port speed and product type. (See the product's installation and service documentation for more information.) Determine the range of values that you can specify by checking the value in the *Limits* column. (For products that have a Buffer Pool, the number of BB_Credits that can be assigned is limited by the number of BB_Credits in the Unallocated Buffers field.)
5. Specify a value in the *RX BB Credit* field or select the *Default* button to populate the *RX BB Credit* fields of all offline ports with the default value appropriate for the port type. As you enter the BB_Credit value, the value is validated against the BB_Credit limits as well as Buffer Pool status. An error message is displayed when applicable. The BB_Credit configuration is not activated if there are any outstanding errors.

6. Click *OK* to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.
7. If the product is offline, set the product online by selecting the *Switch Online* check box on the *Configure* menu.

Configuring NPIV

Node Port Identifier Virtualization (NPIV) is a feature that allows you to assign multiple Fibre Channel addresses (N_port IDs) to a single physical N_port.

The *NPIV* page allows you to enable and disable NPIV logins and to configure the number of NPIV login sessions that are allowed for a port.

NOTE: NPIV is available only if the N_port ID Virtualization feature is installed.

Use the following procedure to configure NPIV functionality:

1. If you are decreasing the number of allowed logins for a port, set the product offline. To set the product offline, clear the *Switch Online* check box on the *Configure* menu.
2. Select *Configure* > *Ports* > *NPIV* on the navigation panel. The *NPIV* configuration page (Figure 3-3) displays.

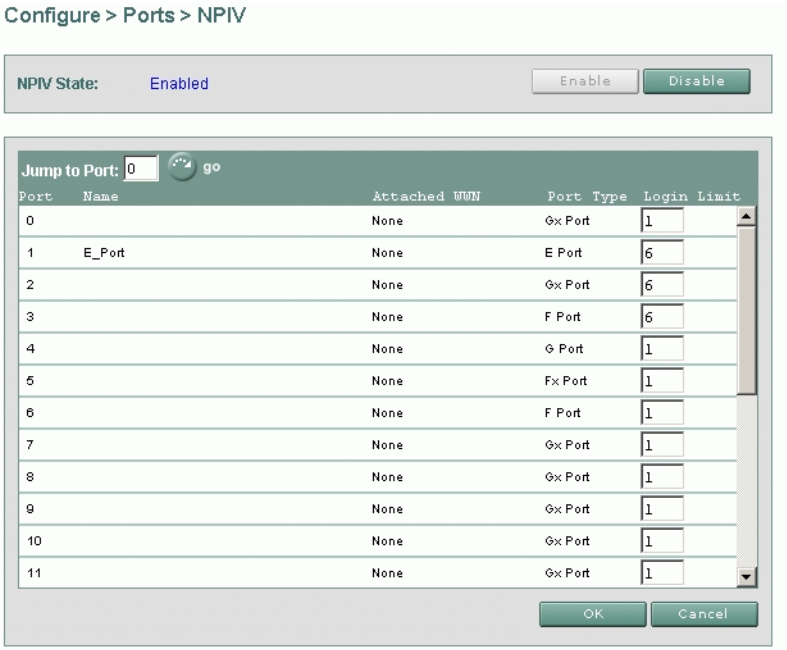

Configure > Ports > NPIV
NPIV State: Enabled
Enable
Disable
Jump to Port: 0
go
Port Name Attached WWN Port Type Login Limit
0 None Gx Port 1
1 E_Port None E Port 6
2 None Gx Port 6
3 None F Port 6
4 None G Port 1
5 None Fx Port 1
6 None F Port 1
7 None Gx Port 1
8 None Gx Port 1
9 None Gx Port 1
10 None Gx Port 1
11 None Gx Port 1
OK
Cancel

Figure 3-3 Port NPIV Configuration Page

3. Enter a value in the *Login* field, to specify the maximum number of login sessions allowed by a product. Valid values are in the range 1 to 256.

   NOTE: You cannot decrease the number of allowed login sessions when the port is online. Set a port offline by blocking it, as described in *Configuring Basic Port Information* on page 3-2.

4. Click *OK* to save and activate the changes. The message **Your changes to the port configuration have been successfully activated** appears.

5. If the product is offline, set the product online by selecting the *Switch Online* check box on the *Configure* menu.

Configuring Switch Information

The task of configuring switch information is available through the following sections:

- *Configuring Switch Identification* on page 3-9
- *Configuring Switch Date and Time* on page 3-10
- *Configuring Switch Parameters* on page 3-11

Configuring Switch Identification

Perform this procedure to configure the product's name, description, location, and contact person. The *Name*, *Location*, and *Contact variables* configured here correspond to variables used by Simple Network Management Protocol (SNMP) management workstations when obtaining data from managed switches or directors. To configure identification:

1. Select *Configure* > *Switch* > *Identification* on the navigation panel. The *Identification* configuration page (Figure 3-4) displays.

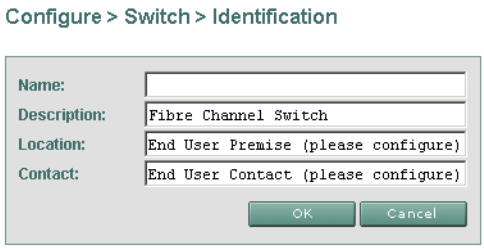


Figure 3-4 Switch Identification Page

2. Type a name in the *Name* field. Each product should be configured with a unique name of 24 or fewer alphanumeric characters.

   If the product is installed on a public LAN, the name should reflect the product's Ethernet network domain name system (DNS) host name. For example, if the DNS host name is **24portswitch.company.com**, the name entered in this dialog box should be *24portswitch*.

TIP: Spaces are allowed in the *Name* field.

3. Type a product description of 255 or fewer alphanumeric characters in the *Description* field.
4. Type the product's physical location (255 or fewer alphanumeric characters) in the *Location* field.
5. Type the name of a contact person (255 or fewer alphanumeric characters) in the *Contact* field.
6. Click *OK* to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.

Configuring Switch Date and Time

Perform this procedure to configure the effective date and time for the product. To set the date and time:

1. Select *Configure* > *Switch* > *Date Time* on the navigation panel. The *Date Time* configuration page (Figure 3-5) displays.

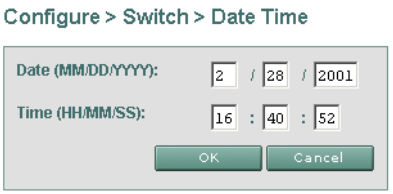


Figure 3-5 Switch Date and Time Page

2. Click the *Date* fields that require change, and type numbers in the following ranges:
   - Month (*MM*): **1** through **12**.
   - Day (*DD*): **1** through **31**.
   - Year (*YYYY*): Greater than **1980**.
3. Click the *Time* fields that require change, and type numbers in the following ranges:
   - Hour (*HH*): **0** through **23**.
   - Minute (*MM*): **0** through **59**.
   - Second (*SS*): **0** through **59**.

4. Click *Activate* to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.

Configuring Switch Parameters

The *Switch Parameters* page is used to enable insistent domain ID, rerouting delay, domain registered state change notifications (RSCNs), suppression of RSCNs during zone set activation, limited fabric RSCNs, and zone FlexPars. The page can also be used to configure a preferred domain ID, switch speed, and interswitch link (ISL) fibre shortest path first (FSPF) cost configuration.

Perform the following procedure to configure switch parameters:

1. If you are going to set the preferred domain ID, switch speed, and ISL FSPF cost configuration, set the product offline. To set the product offline, clear the *Switch Online* check box on the *Configure* menu.
2. Select *Configure* > *Switch* > *Parameters* on the navigation panel. The *Parameters* configuration page (Figure 3-6) displays.

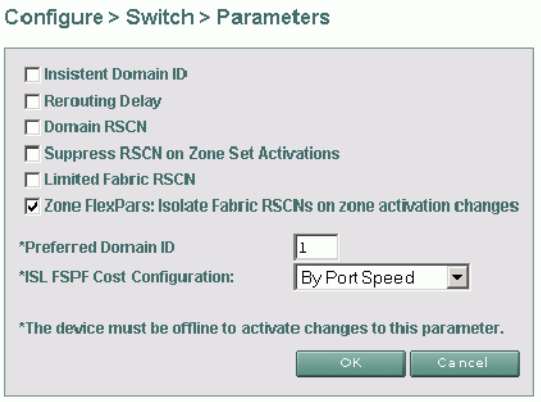


Figure 3-6 Switch Parameters Page

3. Select the *Insistent Domain ID* check box to enable the insistent domain ID. When this check box is filled, the domain ID configured in the *Preferred Domain ID* field becomes the active domain identification when the fabric initializes.

NOTE: If Enterprise Fabric Mode (an optional SANtegrity™ Binding feature) or Fabric Binding is enabled, then *Insistent Domain ID* must be enabled.

4. Select the *Rerouting Delay* check box to enable rerouting delay. When this check box is filled, traffic is delayed through the fabric by the specified error detect time out value (E_D_TOV). This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path. This parameter is only applicable if the product is being configured in a multiswitch fabric.

NOTE: If Enterprise Fabric Mode (an optional SANtegrity™ Binding feature) is enabled, then *Rerouting Delay* must be enabled.

5. Select the *Domain RSCN* check box to enable domain RSCN function. When this check box is selected, messages can be sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. Consult with your HBA and storage device vendor to determine if enabling domain RSCNs will cause problems with your HBA or storage products.

NOTE: If Enterprise Fabric Mode (an optional SANtegrity Binding feature) is enabled, then *Domain RSCN* must be enabled.

6. Select the *Suppress RSCN on Zone Set Activations* check box to suppress sending RSCNs during zone set activations. When this check box is filled, RSCN messages are prohibited from being sent to ports on the switch following any change to the fabric's active zone set. Consult with your HBA and storage device vendor to determine if enabling this parameter will cause problems with your HBA or storage products.
7. Select the *Limited Fabric RSCN* check box to prevent sending fabric RSCNs in case of an Initial Program Load (IPL). When enabled, fabric RSCNs are suppressed after an IPL.
8. Select the *Zone FlexPars: Isolate Fabric RSCNs on zone activation changes* check box to suppress sending fabric-format RSCNs to devices in zones not impacted by the RSCN. As fabrics grow larger, numerous RSCNs from zoning changes can create

congestion and disrupt devices. With zone FlexPars enabled, RSCNs are limited to devices that are impacted by a zoning change.

9. At the *Preferred Domain ID* field, type a value of **1** through **31**. The domain ID uniquely identifies each product in a fabric.

NOTE: If the product is attached to a fabric element, the product and element must have unique domain IDs. If the values are not unique, the E_Port connection to the element cannot carry traffic and the product cannot communicate with the fabric.

---

10. At the *Switch Speed* field, select *1 Gb/sec* or *2 Gb/sec*. This specifies the speed used on the switch. This field is valid only for 64-Port Directors that are able to run at both speeds.

11. At the *ISL FSPF Cost Configuration* field, select *By Port Speed* or *Ignore Port Speed* to configure ISL FSPF cost functionality. This parameter configures the FSPF cost of ISLs on the switch. Cost is a metric assigned to ISLs by the product's Path Selection functionality. Cost is used to determine the shortest path (or the path which would take the least amount of time for traffic to travel) to a destination. A path with a lower cost is considered to be faster than a path with a higher cost. You can specify the following options for this parameter:

    - *By Port Speed*—When selected, the value of the FSPF cost for each port depends on the speed of the port. In this case, the cost is inversely proportional to the bit rate of the ISL. The higher the bit rate, the lower the cost. When this option is specified, the speed of the ISL is a factor in determining the shortest path.
    - *Ignore Port Speed*—When selected, every ISL on the switch has the same FSPF cost. If *Ignore Port Speed* is specified, the number of hops is the primary factor in determining the shortest path; the speed of the ISL is not considered. Select *Ignore Port Speed* for this parameter, if you want parallel ISLs of different speeds to be considered equally as paths for traffic.

TIP: It is recommended that all the switches in the fabric be configured to have the same value for the ISL FSPF Cost Configuration parameter.

12. Click *OK* to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.
13. If fabric parameters require configuration, go to *Configuring Fabric Parameters for the Switch* on page 3-14.
14. If the configuration is complete, set the product online by selecting the *Switch Online* check box on the *Configure* menu.

Configuring Fabric Parameters for the Switch

Perform this procedure to configure the fabric operating parameters, including resource allocation time out value (R_A_TOV), E_D_TOV, product priority, and interop mode. The product must be set offline to configure the parameters.

NOTE: A 12-Port Switch cannot participate in a fabric, unless the Fabric Capable feature is enabled.

Perform the following procedure to configure fabric parameters:

1. Set the product offline by clearing the *Switch Online* check box on the *Configure* menu.
2. Select *Configure* > *Switch* > *Fabric Parameters* on the navigation panel. The *Fabric Parameters* configuration page (Figure 3-7) displays.

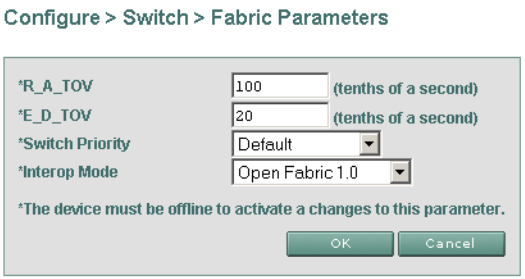


Figure 3-7 Fabric Parameters Page

3. At the *R_A_TOV* field, type a value between **10** and **1200** tenths of a second between 1 and 120 seconds. The R_A_TOV value must be greater than the E_D_TOV value.

NOTE: If the product is attached to a fabric element, the product and element must be set to the same R_A_TOV value. If the values are not identical, the E_Port connection to the element fails and the product cannot communicate with the fabric.

4. At the *E_D_TOV* field, type a value between **2** through **600** tenths of a second (0.2 through 60 seconds). (The E_D_TOV value must be less than the R_A_TOV value.)

NOTE: If the product is attached to a fabric element, the product and fabric element must be set to the same E_D_TOV value. If the values are not identical, the E_Port connection to the element fails and the product cannot communicate with the fabric.

5. Select from the *Switch Priority* drop-down list to set the product priority. Available selections are *Default*, *Principal*, and *Never Principal*. The default setting is *Default*.

   This value designates the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

   Principal is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means the switch is incapable of becoming a principal switch. If all switches are set to *Principal* or *Default*, the switch with the highest priority and the lowest world wide name (WWN) becomes the principal switch.

   At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all interswitch links (ISLs) will segment, causing a failure of connectivity.

6. Select from the *Interop Mode* drop-down list to set the product operating mode. This option does not display if the Operation Mode is S/390[1]. (S/390 Mode is not supported for loop devices.) This setting only affects the mode used to manage the product; it does not affect port operation. Available selections are:

   - **McDATA Fabric 1.0**—Select this option if the product is fabric-attached only to other directors or switches operating in McDATA Fabric 1.0 mode.

- **Open Fabric 1.0**—Select this option for managing heterogeneous fabrics, and if the product is fabric-attached to McDATA directors or switches and open-fabric compliant switches produced by other original equipment manufacturers (OEMs). This setting is the default.

7. Click *OK* to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.
8. If the product is offline, set the product online by selecting the *Switch Online* check box on the *Configure* menu.

Configuring Network Parameters for the Switch

Verify the type of LAN installation with the customer's network administrator. If one McDATA product is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change.

If multiple McDATA products are installed or a public LAN segment is used, network information must be changed to conform to the customer's LAN addressing scheme.

Perform the following steps to change a product's IP address, subnet mask, or gateway address.

1. Select *Configure* > *Switch* > *Network* on the navigation panel. The *Switch Network* configuration page (Figure 3-8) displays.

1. The Operation Mode parameter of the EFCM Basic interface is equivalent to the Management Style parameter of the Element Manager interface of SANavigator. The S/390 Mode used for the EFCM Basic interface is equivalent to the FICON management style on the Element Manager.

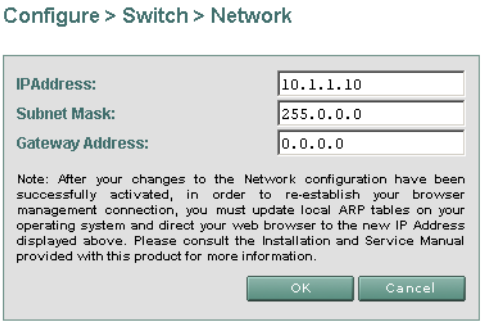

Configure > Switch > Network
IPAddress:
10.1.1.10
Subnet Mask:
255.0.0.0
Gateway Address:
0.0.0.0
Note: After your changes to the Network configuration have been successfully activated, in order to re-establish your browser management connection, you must update local ARP tables on your operating system and direct your web browser to the new IP Address displayed above. Please consult the Installation and Service Manual provided with this product for more information.
OK
Cancel

Figure 3-8 Switch Network Configuration Page

a. At the *IP Address* field, type the new value specified by the customer's network administrator (default is **10.1.1.10**).

b. At the *Subnet Mask* field, type the new value specified by the customer's network administrator (default is **255.0.0.0**).

c. At the *Gateway Address* field, type the new value specified by the customer's network administrator (default is **0.0.0.0**).

2. Click *OK* to save and activate the changes.
3. Update the address resolution protocol (ARP) table for the browser PC. Delete the product's ***old*** IP address from the ARP table using the process that is appropriate for the operating system (OS) in use by the system.
4. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
5. At the browser, enter the product's ***new*** IP address as the Internet URL. The *Enter Network Password* dialog box displays.
6. Type the user name and password.

NOTE: The default user name is **Administrator** and the default password is **password.** The user name and password are case-sensitive.

---

7. Click *OK*. The EFCM Basic interface opens.

Configuring SNMP

Perform this procedure to enable the SNMP agent, configure community names, write authorizations, network addresses, and user datagram protocol (UDP) port numbers for up to six SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs. To configure SNMP trap recipients:

1. Select *Configure* > *SNMP* on the navigation panel. The *SNMP* configuration page (Figure 3-9) displays.

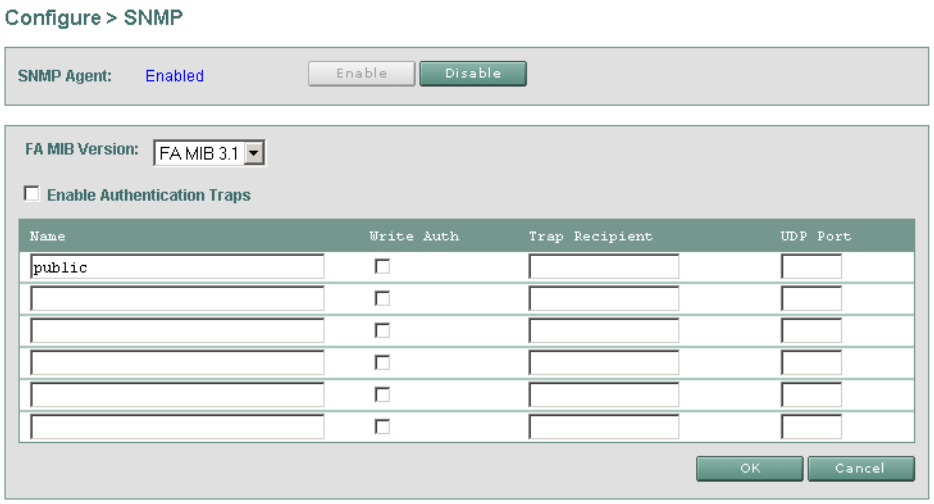


Figure 3-9 SNMP Configuration Page

2. Click the *Enable* button to enable the SNMP Agent. To disable the SNMP Agent, select the *Disable* button.
3. Select a Fibre Alliance Management Information Base (FA MIB) version in the *FA MIB Version* field. The options are *FA MIB 3.0* and *FA MIB 3.1*. This should be set to match the level of FA MIB used by the SNMP management stations that access the product.
4. Select the *Enable Authentication Traps* check box to enable authentication trap messages to be sent to SNMP management stations when unauthorized stations try to access SNMP information from the product. Clear the check box to disable authorization trap messages.

5. For each trap recipient to be configured, type a community name of 32 or fewer alphanumeric characters in the *Name* field. The community name is incorporated in SNMP trap messages to prevent unauthorized viewing or use. Duplicate community names are allowed, but the corresponding Write Authorization check boxes must match.

TIP: Spaces are allowed in the *Name* field.

6. Click the check box in the *Write Auth* column to enable or disable write authorization for the trap recipient (default is disabled). A check mark indicates write authorization is enabled. When the feature is enabled, a management workstation user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.
7. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the *Trap Recipient* field in four-byte, dotted-decimal format with a maximum of 16 characters. It is recommended the IP address be used.
8. The default UDP port number for trap recipients is **162**. Type a decimal port number in the *UDP Port* field to override the default. The range for the UDP port number value is 1 to 65535.
9. Click *OK* to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.

Configuring CLI and SSH

Perform this procedure to enable (activate) or disable (deactivate) the state of the product's command line interface (CLI), as well as to configure the secure shell (SSH), which is used to provide secure access and encrypted data when using the SSH function. To enable or disable CLI as well as enable SSH, use the procedures that follow:

1. Select *Configure* > *CLI* on the navigation panel. The *CLI* configuration page (Figure 3-10) displays.

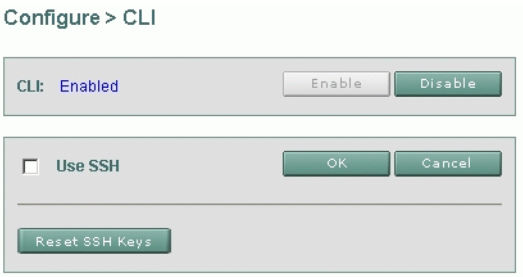


Figure 3-10 CLI Configuration Page

2. Select the *Enable* button to enable the CLI. Select the *Disable* button to disable the CLI.
3. Enable SSH by selecting the *Use SSH* check box. Disable SSH by clearing the check box. Click *OK* to activate the SSH change.

NOTE: The default method is Telnet, which means that data is not encrypted between the user and the product. By enabling SSH, data, such as the user ID and password, is encrypted between the user and the product. It is recommended that you enable SSH to ensure that data such as user IDs and passwords are encrypted when users use Telnet to access a product. Also, if you enable SSH, Telnet function is disabled.

---

4. If you need to reset the SSH host public/private keys, select the *Reset the SSH Keys* button.

NOTE: Resetting the SSH host public/private keys is a task that should be performed based on your company's Information Technology (IT) policy. When you reset the keys, you reset both the public and private keys. Resetting the keys is usually performed if there is a concern that the keys have been compromised or if your company's IT policy requires the keys to be reset on a regular basis. Do not reset the keys unless you have consulted with or been instructed to by your network administrator.

Configuring OSMS and Host Control

Perform this procedure to enable or disable OSMS and host control of the product through EFCM Basic.

OSMS is a feature that allows host control and inband management of the director or switch through a management application that

resides on an open-systems interconnection (OSI) device. This device is attached to a director or switch port. The device communicates with the switch or director through Fibre Channel common transport (FC-CT) protocol.

Use the following procedure to configure OSMS and host control:

1. Select *Configure* > *OSMS* on the navigation panel. The *OSMS* configuration page (Figure 3-11) displays.

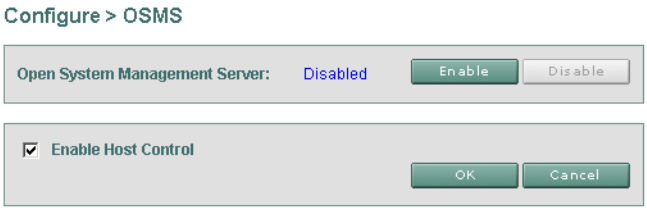


Figure 3-11 OSMS Configuration Page

2. Select the Enable button to enable OSMS management of the product through an open-systems interconnection (OSI) device. Select the Disable button to disable OSMS management of the product.
3. Enable host control on the product by selecting the *Enable Host Control* check box. (To enable host control, OSMS management must be enabled.) Disable host control by clearing the check box. Select the *OK* button to activate your change.

Configuring SSL

The *SSL* configuration page provides you with the ability to configure the Secure Sockets Layer (SSL). SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a public-and-private key encryption system, which includes the use of a digital certificate. The certificate enables a server to be authenticated.

The SSL configuration page is divided into the following sections:

- **Enable/Disable section**—Provides the ability to enable and disable Web SSL and Software SSL.

- **Current Certificate Details**—Provides current information related to SSL certificates. This part of the page shows the following items:
  - The public certificate. The same certificate is used for both web and software connections. The certificate contains public information that is not secret. (The certificate has a private counterpart, the SSL private key, which is kept secret and is not displayed.)
  - The MD5 fingerprint of the certificate. This is the fingerprint of the certificate using the Message Digest 5 (MD5) algorithm. The user can compare the fingerprint here with the fingerprint provided by the web browser to ensure that they match.
  - SHA-1 fingerprint certificate. This is the fingerprint of the certificate using the SHA-1 algorithm. The user can compare the fingerprint here with the fingerprint provided by the web browser to ensure that they match.

NOTE: Browsers can supply the MD5 fingerprint, the SHA-1 fingerprint, or both.

- **New Certificate**—Enables you to generate a new certificate and identify the expiration period for the certificate.
- **SSL Renegotiation**—Enables you to define parameters for renegotiation of the certificate.

Use the following procedures to configure SSL certificates:

1. Select *Configure* > *SSL* on the navigation panel. The *SSL* configuration page (Figure 3-12 on page 3-24) displays.
2. To enable or disable Web SSL, click the corresponding *Enable* and *Disable* buttons. When enabled, all data sent over a web connection is encrypted. When disabled, no data sent over the connection is encrypted.

NOTE: Once Web SSL is enabled, the user is forced to log in again, and accept, reject, or import the security certificate.

TIP: A connection to a product that has Web SSL enabled is established by specifying `https` at the beginning of the URL. If only `http` is used, the connection is automatically redirected to the URL beginning with `https`.

3. To enable or disable Software SSL, click the corresponding *Enable* and *Disable* buttons. The state of Software SSL controls the ability of a program to use an Application Program Interface (API) to connect. If Software SSL is disabled, the secure API connection is rejected. If Software SSL is enabled, both secure and non-secure connections are accepted; however, the non-secure connection is immediately redirected to a secure connection so that all API communication is encrypted.
4. To define the expiration period for the certificate, enter a value in the *Expires in* field. The number of days for the expiration is in the range of 30 to 3650 days. The default value is 365 days.
5. To generate a new certificate, select the *Generate* button. The certificate information displays in the *Current Certificate Details* field.
6. To define parameters for the renegotiation of the SSL session key, enter a value in the *Renegotiate after* field of the *SSL Renegotiation* area. This value defines the number of megabytes (MB) of data that pass over the connection that triggers regeneration of the SSL session key. (An SSL session key is valid only for the life of an individual SSL connection, until it is renegotiated per the value of this parameter. The SSL session key is not part of the certificate.) Valid values for the parameter are 50 MB to 1000 MB. If set to 0, SSL session key renegotiation is turned off. Select the OK button to activate this parameter.

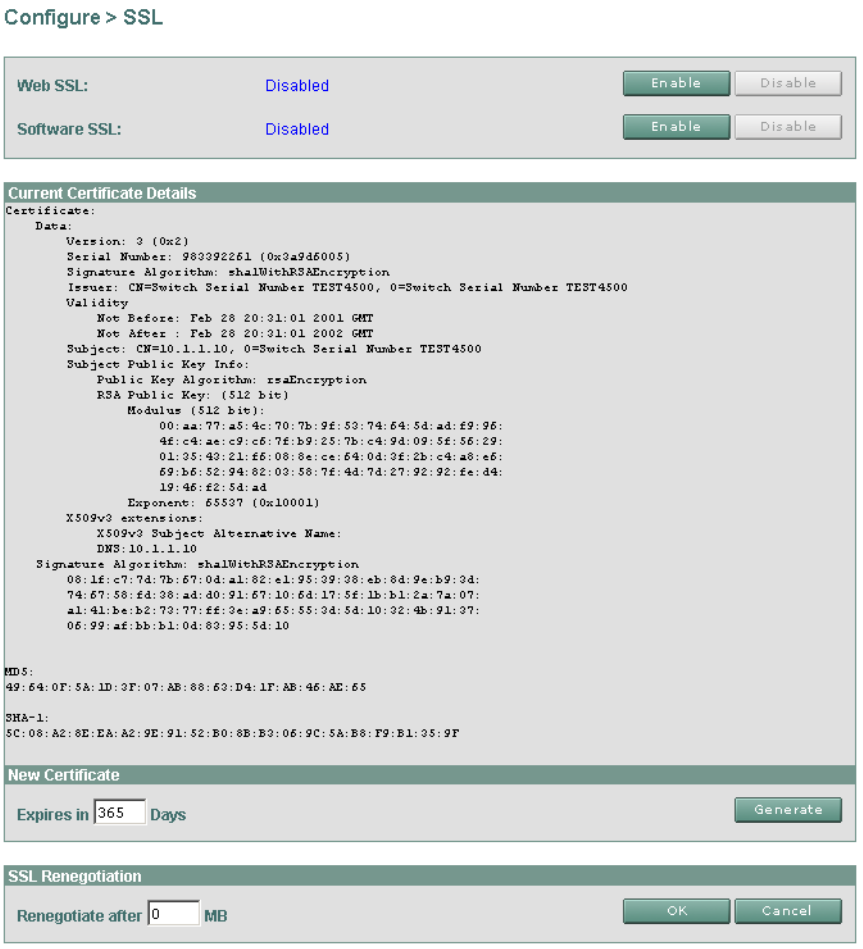


Figure 3-12 SSL Configuration Page

Zoning

A description of use of the *Zoning* page and of the topic of zoning is found in Chapter 4, *Configuring Zoning*.

Configuring Performance Parameters

The following sections describe how to configure performance parameters:

- *Configuring Open Trunking* on page 3-25
- *Configuring Preferred Paths* on page 3-27

Configuring Open Trunking

The *Open Trunking* page enables you to configure open trunking settings. OpenTrunking is an optional software feature that is enabled using a feature key.

The purpose of open trunking is to make efficient use of redundant interswitch links (ISLs) between neighboring switches by means of load balancing. ISLs are fiber optic cables that connect ports between Fibre Channel switches and link these switches into a multiswitch fabric. Fibre Channel traffic flows through these ISLs from end devices (servers and storage devices) attached to ports on individual switches.

When the traffic on a particular port exceeds a specified threshold, the open trunking functionality routes some of the traffic to another ISL. This prevents traffic from becoming congested on an ISL. Open trunking provides automatic, dynamic, statistical traffic load balancing across ISLs in a fabric environment.

The OpenTrunking feature monitors Fibre Channel data rates through multiple ISLs, dynamically applies a fibre shortest path first (FSPF) networking algorithm to calculate the optimum path between fabric elements, and balances the Fibre Channel traffic load accordingly. The objective is to make the most efficient possible use of redundant ISLs between neighboring switches, even if these ISLs have different bandwidths.

The OpenTrunking feature monitors the average data rates of all traffic flows, from a transmit port to a destination domain. It periodically adjusts routing tables to reroute data flows from congested links to lightly loaded links and optimize bandwidth use.

Load balancing among the ISLs does not require user configuration, other than enabling open trunking and selecting optional or default settings for congestion thresholds (per port) and a response threshold for lack of BB_Credits. In particular, you do not need to manually configure ISLs into trunk groups of redundant links where data can

be off-loaded. Candidate links for rerouting flow are identified automatically and maintained by the FSPF protocol. All ISLs that lead to adjacent switches on the shortest path to the flow's destination are considered. This means that even if a link is not on the shortest path to the destination, the flow may be rerouted to this link to relieve congestion. This also means that flow may be rerouted onto a link that goes to a different adjacent switch.

Configuring Open Trunking Values

To configure open trunking:

1. Select *Configure* > *Performance* > *Open Trunking* on the navigation panel. The *Open Trunking* configuration page (Figure 3-13) displays.

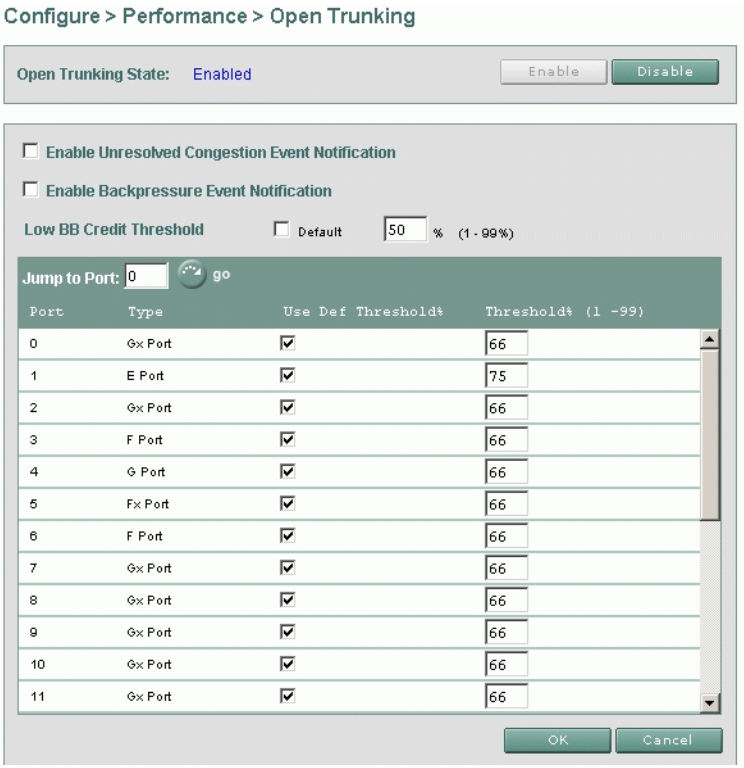


Figure 3-13 Open Trunking Page

2. Select the Enabled button to enable open trunking. Select the Disable button to disable open trunking. (These actions take effect immediately.)

3. Unresolved congestion occurs when a flow cannot be rerouted to another link because it would exceed the other link's threshold. Select the *Unresolved Congestion Event Notification* check box to enable unresolved congestion event notification. If enabled, an unresolved congestion entry is made in the event log and, if SNMP is configured, an SNMP trap is generated. To disable this function, clear the check box.
4. Backpressure occurs when the threshold of unavailable BB_Credits is exceeded for any link. Select the *Backpressure Event Notification* check box to enable backpressure event notification. If enabled, a backpressure entry is made in the event log and, if SNMP is configured, an SNMP trap is generated. To disable this function, clear the check box.
5. Specify a value for the *Low BB Credit Threshold* parameter, if desired. The system monitors the percentage of time that the port experiences no transmit BB_Credits on the link. The link cannot transmit without BB_Credits. When the threshold is exceeded, the system reroutes flows away from the ISL that is experiencing this problem. This threshold is also used to prevent rerouting of traffic to an ISL that is experiencing a low BB_Credit threshold condition. Select the *Default* check box to specify that the default threshold value of 10% should be used rather than the value in the % entry field. This parameter must be a value in the range 1 to 99, if the *Default* check box is cleared.
6. Specify a load-balancing threshold value in the *Threshold* field for each port, if desired. Use this field to configure the value of the load-balancing threshold for each port. When this threshold is exceeded, the open trunking functionality offloads some of the traffic to another ISL. Select the *Use Def Threshold* check box to specify that default threshold value of 10% should be used rather than the value in the *Threshold* field. The *Threshold* must be a value in the range 1 to 99, if the *Use Def Threshold* check box for the port is cleared.

Configuring Preferred Paths

The preferred path feature enables you to prioritize ISLs for a selected port on the switch. The preferred path capability customizes the static load-balancing function by enabling you to specify an ISL preference for each remote domain. Preferred Path, however, is still subject to the standard Fabric Shortest Path First (FSPF) requirements, which allow the firmware to override the configuration setting if errors are encountered.

The data path consists of the source port of the switch or director being configured, the exit port of that switch or director, and the domain ID of the destination switch or director. Each switch or director must be configured for its part of the desired path in order to achieve optimal performance. You may need to configure Preferred Paths for all switches or directors along the desired path for a proper multi-hop Preferred Path. (For examples of Preferred Path implementation and other related information, see your product's Element Manager manual.)

The following rules apply when configuring Preferred Paths:

- The switch's domain ID must be set to insistent.
- Domain IDs must be in the range of 1 through 31.
- The specified numbers for source ports and exit ports must be in the range equal to the number of ports for the switch being configured.
- For any source port, only one path may be defined to each destination domain ID.

Use the following procedure to configure preferred paths:

1. Select *Configure* > *Performance* > *Preferred Path* on the navigation panel. The *Preferred Path* configuration page (Figure 3-14) displays.

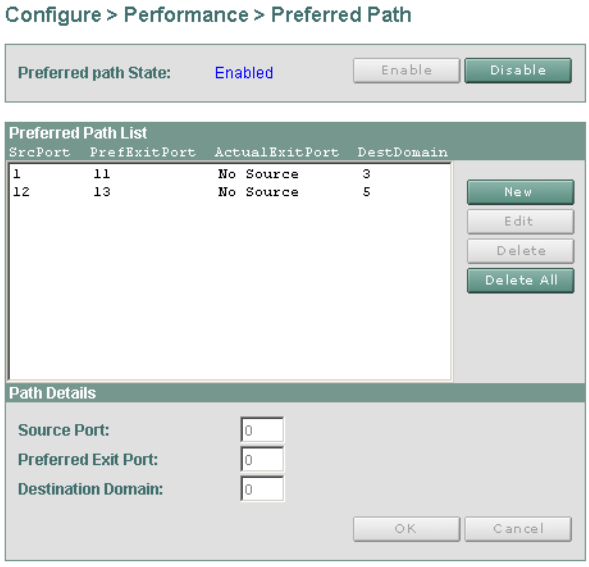


Figure 3-14 Preferred Path Page

2. Select the *Enable* button to enable Preferred Path function. Select the *Disable* button to disable preferred path function. When the Preferred Path configuration state is disabled, the switch will not use the configured Preferred Paths. If it is enabled, then it will use the configured Preferred Paths.
3. The *Preferred Path List* shows the currently configured preferred paths. You can configure this list as follows:
   a. Click the *New* button to add a new preferred path to the list. The *Path Details* dialog is enabled. Enter values for the following fields:
      - Source Port—The source port of the traffic.
      - Preferred Exit Port—The port to be used for traffic being sent to the destination product.
      - Destination Domain—The domain ID of the destination product. This must be a valid domain ID in the range **1** to **31**.

      Select the *OK* button to add your entry to the list.

b. To edit an existing path, select it from the list, then click the *Edit* button. The information for the selected path is populated in the *Path Details* dialog. Change the desired fields and select the *OK* button to show your changes in the list.

c. To remove a path from the list, select it and click the *Delete* button. The path is deleted from the list. You can also select the *Delete All* button to remove all paths from the list.

Changes to the *Preferred Path List* are activated immediately on the product.

Configuring Port Fencing

The *Port Fencing* page enables you to configure the Port Fencing policies for the product.

Port Fencing is a policy-based feature that allows the user to set thresholds on various types of port events. If the port generates more events than a threshold limit in a user-specified time period, the Port Fencing feature blocks the port, disabling transmit and receive traffic until the user has a chance to investigate, solve the problem, and manually unblock the port.

The *Port Fencing* page has two parts:

- Policies—This list shows the existing Port Fencing policies and allows the user to add, edit, delete, enable, and disable policies.
- Policy Details—This part of the page enables the user to configure policies.

Use the following procedure to configure Port Fencing:

1. Select *Configure* > *Port Fencing* on the navigation panel. The *Port Fencing* configuration page (Figure 3-15) displays.

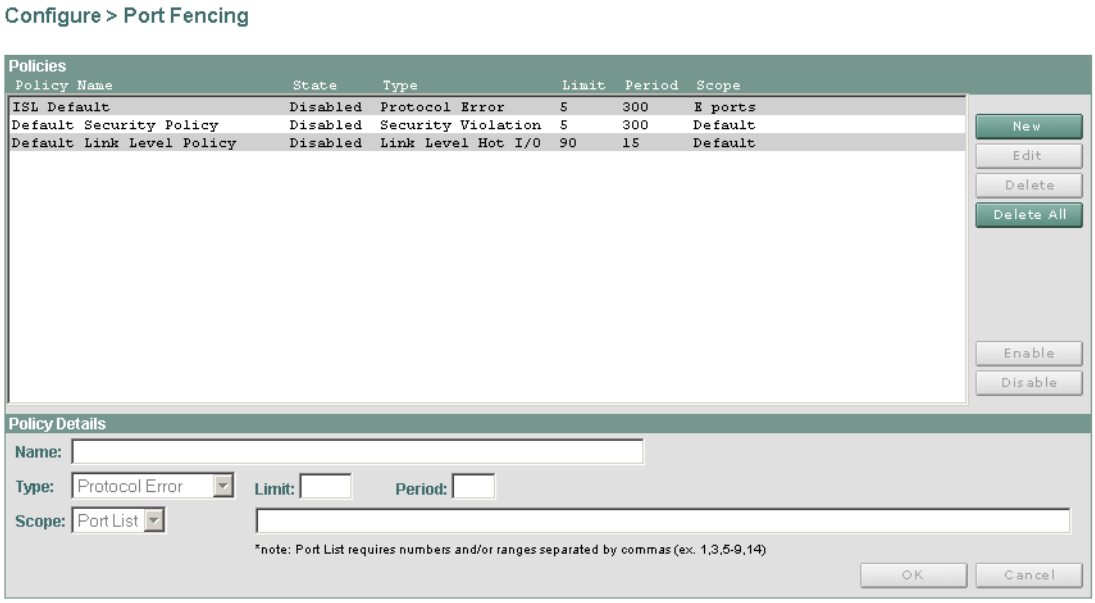


Figure 3-15 Port Fencing Page

2. To enable a policy, select a policy from the *Policy Name* column and select the *Enable* button. To disable a policy, select a policy from the *Policy Name* column and select the *Disable* button.
3. Configure policies using any of the following methods:
   a. Add a new policy by selecting the *New* button. Specify the details of the policy in these fields:
      - *Name*—Specify a name for the policy.
      - *Type*—Select an event type for the fencing policy from the drop-down list.
      - *Limit*—Specify the number of events to serve as the threshold that triggers blocking a port.
      - *Period*—Specify the time interval, in seconds, for the counting of events. If the value specified for *Limit* is exceeded in this time period, the port is blocked.
      - *Scope*—Specify the ports to which the policy applies. Select the type of port from the drop-down list. Values include *E Ports*, *F Ports*, *FL ports*, *Default*, and *All Ports*. Or specify a

list of ports by number by selecting *Port List* from the drop-down list and listing the ports in the entry field. (Identify the ports by port number, or port range, separated by commas. For example, **1,3,5-9,14**.)

Select the *OK* button to add your new policy to the Policies List. The message **Your changes have been successfully activated** displays below the page's heading.

b. Edit an existing policy by selecting it from the Policies List and selecting the *Edit* button. Make the desired changes in the *Policy Details* area. Select the *OK* button to populate your changes to the Policies List. The message **Your changes have been successfully activated** displays below the page's heading.

NOTE: A policy cannot be changed while it is enabled. You must disable a policy to change it.

4. Delete a policy by selecting it from the Policies List and selecting the *Delete* button. Or delete all disabled policies by selecting the *Delete All* button. The message **Your changes have been successfully activated** displays below the page's heading.

NOTE: A policy cannot be deleted while it is enabled. You must disable a policy to delete it.

Setting a Switch Online and Offline

Many configuration changes require that the product be offline. You can set the product online or offline using a check box on the *Configure* menu (Figure 3-16).

To set the product online, select the *Switch Online* check box on the *Configure* menu. To set the product offline, clear the *Switch Online* check box on the *Configure* menu.

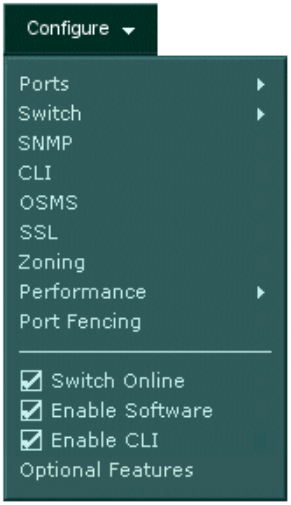


Figure 3-16 Configure Menu

Enabling and Disabling Software

Perform this procedure to enable and disable the ability of software other than E/OS to control the product. Examples of software that are affected by this are SAN management interfaces, such as EFC Manager, and APIs, such as the SMI-S Interface.

To enable software, select the *Enable Software* check box on the *Configure* menu (Figure 3-16 on page 3-33). To disable software, clear the *Enable Software* check box on the *Configure* menu.

Enabling and Disabling the CLI

Perform this procedure to enable (activate) or disable (deactivate) the product's command line interface (CLI). The CLI is alternative to Graphical User Interface (GUI) and web-based (HTTP) interface products for product management.

To enable the CLI, select the *Enable CLI* check box on the *Configure* menu (Figure 3-16 on page 3-33). To disable the CLI, clear the *Enable CLI* check box on the *Configure* menu.

Upgrade Options

For information about the *Upgrade Options* command on the *Configure* menu, see *Adding Licensed Features* on page 9-2.

4

Configuring Zoning

This section describes the concepts of zoning and provides procedures for using the EFCM Basic interface to create and manage zones.

- *Understanding Zoning* *4-1*
- *Using The Zoning Page* *4-13*
- *Creating and Modifying a Zone* *4-14*
- *Configuring the Zone Set* *4-17*

Understanding Zoning

Designing zoning can be complex, especially for multiswitch fabrics. Consult your managed-product vendor's professional services organization before configuring zoning.

This section is designed to help you understand the following concepts so that you can more efficiently use EFCM Basic features to configure and manage zones across a multiswitch fabric:

- How zoning works to control access to storage devices and servers across a fabric
- Other methods of controlling access at the switch and at the server and device, such as binding
- Merging zoned fabrics
- Basic terms and concepts of zoning that you must understand when configuring zoning

Controlling Access Across a Fabric

Zoning features enable you to establish zoning across a fabric of devices attached to switches and directors by partitioning these devices into groups called zones. A zone is composed of devices that can access each other through port-to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.

System administrators create zones to increase security measures and prevent data loss or corruption by controlling access between devices (such as servers and data storage units), or between separate user groups (such as engineering or human resources). Zoning allows an administrator to:

- Establish barriers between devices that use different operating systems. For example, it is often critical to separate servers and storage devices with different operating systems because accidental transfer of information from one to another can delete or corrupt data. Zoning prevents this by grouping devices that use the same operating systems into zones.
- Create logical subsets of closed user groups. Administrators can authorize access rights to specific zones for specific user groups, thereby protecting confidential data from unauthorized access.
- Create groups of devices that are separate from devices in the rest of a fabric. Zoning allows certain processes (such as maintenance or testing) to be performed on devices in one group without interrupting devices in other groups.
- Allow temporary access between devices for specific purposes. Administrators can remove zoning restrictions temporarily (for example, to perform nightly data backup), then restore zoning restrictions to perform normal processes.

Figure 4-1 illustrates three zones established on a single managed product with four devices in each zone. Devices in each zone can communicate with and access devices only in their respective zones.

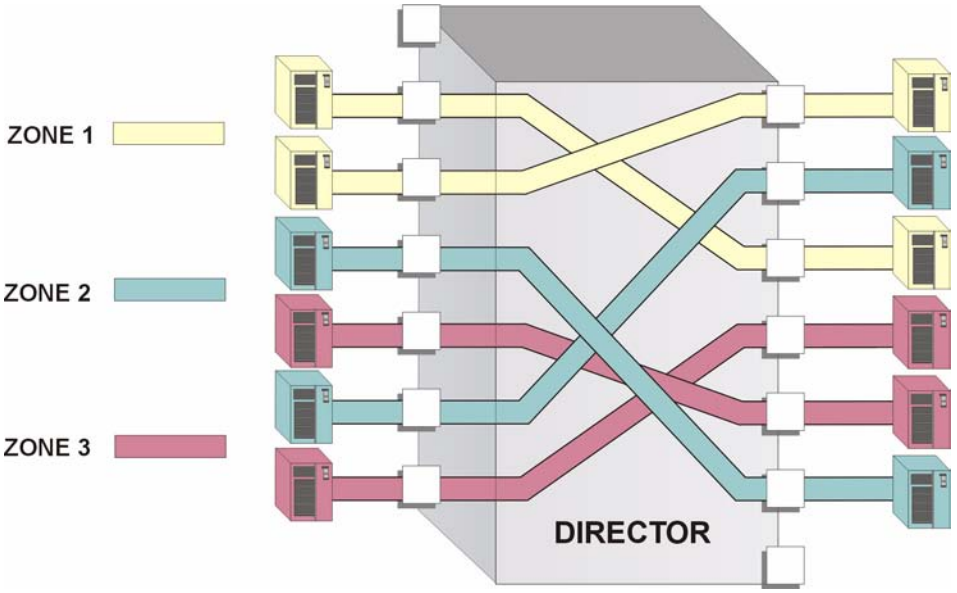


Figure 4-1 Zoning through a Single Fibre Channel Managed Product

Figure 4-2 illustrates how zones can consist of ports and (or) devices installed on ports in three managed products in a multiswitch fabric.

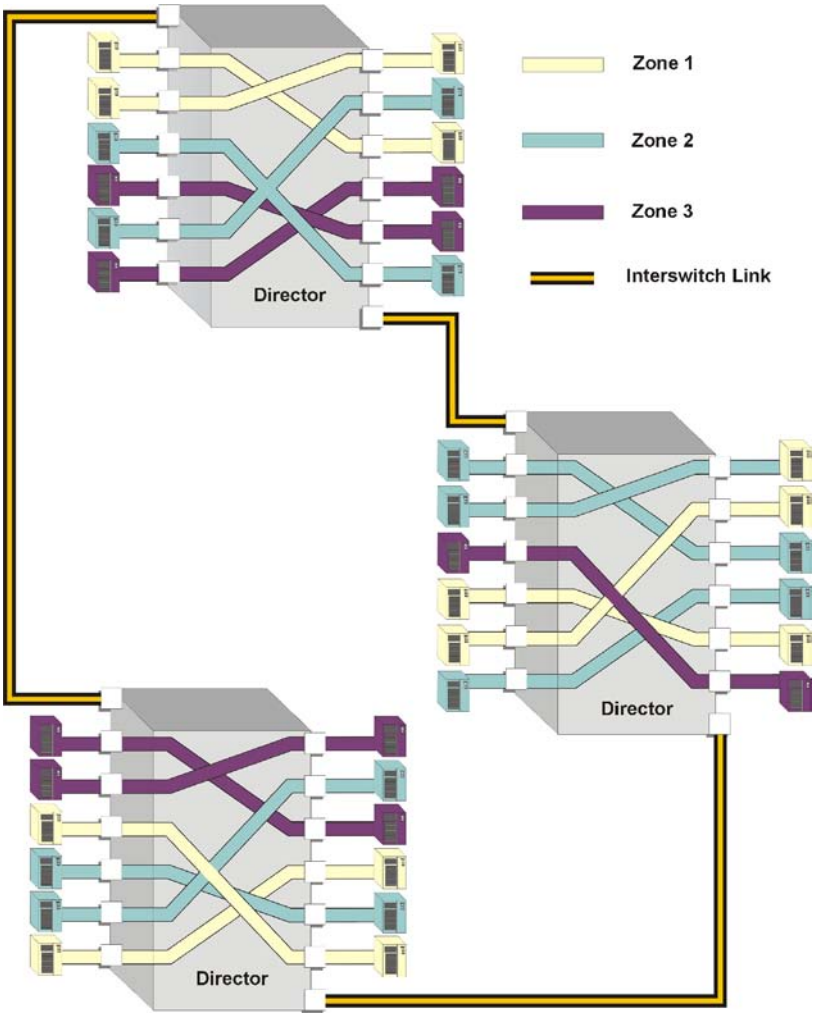


Figure 4-2 Zoning Through a Multiswitch Fabric

Controlling Access at the Switch

A port binding feature is available on switches and directors that allows you to "bind" a specific switch or director port to the world wide name (WWN) of an attached device for exclusive communication. This Port Binding feature is available through the the *Port Binding* command, under the *Security* menu (see *Configuring Port Binding* on page 5-33).

Controlling Access at the Server or Storage Device

Features available at the server or storage device can add methods beyond zoning to increase network security measures, differentiate between operating systems, and prevent data loss or corruption by controlling access between devices or between separate user groups (such as engineering or human resources).

Server-level access control is called persistent binding. Persistent binding uses configuration information stored on the server and is implemented through the server's host bus adapter (HBA) driver. The process binds a server device name to a specific Fibre Channel storage volume or logical unit number (LUN), through a specific HBA and storage port WWN. In essence, this feature creates a reliable route across the fabric that sustains the small computer system interface (SCSI) connection between a server and storage device.

For persistent binding:

- Each server HBA is explicitly bound to a storage volume or LUN, and access is explicitly authorized (access is blocked by default).
- The process is compatible with open system interconnection (OSI) standards. The following are supported:
  - — Different operating systems and applications.
  - — Different storage volume managers and file systems.
  - — Different fabric devices, including disk drives, tape drives, and tape libraries.
- If the server is rebooted, the server-to-storage connection is automatically re-established.
- The connection is bound to a storage port WWN. If the fiber-optic cable is disconnected from the storage port, the server-to-storage connection is automatically re-established when the port cable is reconnected. The connection is also automatically re-established if the storage port is cabled through a different managed product port.

Access can also be controlled at the storage device as an addition or enhancement to redundant array of independent disks (RAID) controller software. Data access is controlled within the storage device, and server HBA access to each LUN is explicitly limited (access is blocked by default). Storage-level access control:

- Provides control at the storage port and LUN level, and does not require configuration at the server.
- Is typically proprietary and protects only a specific vendor's storage devices. Storage-level access control may not be available for many legacy devices.

Before establishing persistent binding or access control features at the storage device, consult with your managed-product vendor's professional services organization.

Zoning Concepts

Zoning is configured by authorizing or restricting access to name server information associated with device ports that attach to product ports. A zone member is specified by the number of the product port to which a device is attached, or by the 8-byte WWN assigned to the HBA or Fibre Channel interface installed in a device. A device port can belong to multiple zones.

Zoning concepts include:

- Zones
- Default zone
- Zone sets
- Active zone set

Naming Conventions for Zones and Zone Sets

The following naming conventions apply to zones and zone sets:

- All names must be unique and may not differ by case only. For example, myzone and MyZone are both valid individually, but they are not considered to be unique.
- The first character of a zone set name must be a letter (A-Z, a-z).
- A zone set name cannot contain spaces.
- Valid characters are a-z, A-Z, 0-9, ^, -, _, and $.
- A zone set name can have a maximum of 64 characters.

Zones

A zone comprises a set of members that can access each other. Refer to Table 4-1 on page 4-10 for details on the number of members that you can configure in a zone and the number of zones that you can configure with the Configure Zone functions.

A zone member can be a switch or director port or the WWN of the device. Ports and devices spread throughout multiple managed products in a multiswitch fabric may be grouped into the same zone. Members of a zone can see each other; members in different zones cannot. The number of members that you can configure for a zone varies according to the number of zones in the zone set, the length of the zone names, and other factors, but is essentially bounded by the available nonvolatile random-access memory (NVRAM) in the managed product. See Table 4-1 on page 4-10 for various parameter limits that affect how you configure zones.

NOTE: Port numbers cannot be used for zone members if the interoperability mode for the switch or director is set to Open Fabric 1.0 mode. In this case, you must use node WWNs as zone members.

The type of zone members identified for a zone may be mixed and matched. For example, two members may be specified by a port number and the third member by the WWN of the device.

Using WWNs

To identify a zone member by WWN, use the 16-digit WWN of the device. For example:

10:00:08:00:88:40:C0:D4

In the EFCM Basic interface, the WWN displays with the switch or director manufacturer's name before the WWN. The WWN is assigned to the Fibre Channel interface or HBA installed in devices

such as servers or storage devices. Although the device may also have a *node* WWN, this WWN is not used for zoning identification.

NOTE: Nicknames can be assigned to the WWN using the Element Manager. This functionality is not available in EFCM Basic.

The advantage of identifying a zone member as the WWN of the attached device is that the identification will not change if fiber cable connections to ports are rearranged. This is especially important if you are using spare ports. You can simply move the fiber cable to a spare port from a failed port and still maintain the zoning configuration.

The disadvantage of identifying a zone member by the WWN is that removal and replacement of a device HBA or Fibre Channel interface (thereby changing the device WWN) disrupts zone operation and may incorrectly include or exclude a device from a zone.

Using Port Numbers

To identify a zone member by port number, use the domain identification number of the managed product and the port number on that managed product. For example:

Domain 1, Port 1

NOTE: Port numbers cannot be used for zone members if the Interoperability mode for the switch or director is set to Open Fabric 1.0 mode.

Port numbers can be 0 through *n*, with *n* representing the number of ports on the managed product minus one. When you define a zone member by a port number, any device attached through that port is included in the zone. A port number that you assign as a zone member is automatically prefixed with the domain identification number of the managed product.

The advantage of identifying a zone member by port number is that if the HBA on an attached device fails, you don't have to identify the member with the WWN of the replacement HBA.

A disadvantage of port zoning is that someone may rearrange cable connections to ports (because of port failures or other reasons) and inadvertently allow devices to communicate that should not have access to each other.

NOTE: If a managed product's Domain ID changes, you must reconfigure all zones that contained the managed product's port as a zone member. We recommend assigning unique Preferred Domain IDs to each switch in the fabric using the *Switch Parameters* page to change the Preferred Domain IDs (see *Configuring Switch Parameters* on page 3-11).

Default Zone

A default zone consists of all devices that have not been configured as members of a zone in a currently-active zone set. Remember:

- You can enable or disable the default zone separately from the active zone set by selecting the *Zoning* command from the *Configure* menu. Enabling the default zone allows all devices and ports not configured as members of the active zone set to communicate. If the default zone is disabled, these ports and devices cannot communicate.
- If no zone set is activated, then all devices are considered to be in the default zone.
- If a zone set is active, then all connected devices that are not included as a members of a zone in the active zone set are included in the default zone.

Zone Sets

A zone set is a group of zones that you can activate or deactivate as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time. Devices that are members of zones in the zone set can only communicate with members of zones in the same zone set. However, devices can be included as members of more than one zone set. By activating a zone set, you are making all zones in the set active.

Table 4-1 on page 4-10 shows the limits for configuring zoning in McDATA fabrics that are supported by switch and director firmware. Although the EFCM Basic interface or other interfaces may allow you to configure greater values, values in this table have been tested and are supported. For the latest limits, refer to the *Supported Fabrics Configuration Document* located on www.mcdata.com in the Resource Library or contact your customer support representative.

Table 4-1 Zone Set Configuration

Zone Set Configuration	Limit
Number of members in a zone	4096
Number of unique zone members in a zone set	4096
Number of zone members in a zone set, including duplicates	8192
Number of zones in a zone set	2048 (2047 plus the default zone)
Characters per zoning name	64

Consider the following factors when configuring zone sets for your system:

- If no zone set is active, and the default zone is disabled, then no devices can communicate.
- If you activate a zone set when there is already an active zone set, that set will replace the currently active zone set.
- If you deactivate the current active zone set, then all devices connected in the fabric become members of the default zone.

Active Zone Set

An active zone set is a zone set that is currently active on a single-switch fabric or across all managed products in a multiswitch fabric. At any time, you can disable zoning by deactivating the active zone set and enabling the default zone, or you can enable zoning by activating a zone set. When a zone set is active, all zones that are members of that zone set are active. Only one zone set can be active for the fabric at one time. If no zones are active, then all devices are considered to be in the default zone.

Merging Zoned Fabrics

Managed products are linked through Interswitch Links (ISLs) to form multiswitch fabrics. In a multiswitch fabric, the active zoning configuration applies to the entire fabric. Any change to the configuration applies to all switches in the fabric.

When fabrics join through an ISL, adjacent managed products exchange active zone configurations and determine if the configurations are compatible and can merge. Zoning configurations are compatible if the active zone names in each fabric are unique. If there are identical zone names in each fabric, then the zones must have identical members for the fabrics to join.

If the configurations can merge, the fabrics join. The resulting configuration will be a single zone set containing zone definitions from each fabric.

If configurations cannot merge, the expansion ports (E_Ports) on each product become segmented. Segmented E_Ports cannot carry traffic from attached devices (class 2 or 3 traffic), but can carry management and control traffic (class F traffic) between managed products.

Rules for Merging Zoned Fabrics

Certain rules are enforced to ensure that zoning is consistent across the fabric. Table 4-2 on page 4-12 summarizes rules for joining two fabrics through an ISL. The following terms are used in the table:

- **Not zoned**—No zone set is active in the fabric and the default zone is enabled. All devices in the fabric are visible to all other devices in the fabric.
- **Zoned**—A zone set is active in the fabric and/or the default zone is disabled. Devices can discover other devices that are members of the same zone.
- **Zoning configuration**—Combination of the active zone set definition and the default zone state (enabled or disabled).

Table 4-2 Merging Zones

Fabric A	Fabric B	Result
Not zoned	Not zoned	Fabrics join successfully. The new fabric remains not zoned.
Not zoned	Zoned	Fabrics join successfully and the active zone set will propagate across the fabric. Fabric A inherits zoning configuration from Fabric B.
Zoned	Not zoned	Fabrics join successfully and the active zone set will propagate across the fabric. Fabric B inherits zoning configuration from Fabric A.
Zoned	Zoned	Fabrics can merge if the zone names in each fabric are unique. The resulting active zone set is a union of the zones from each fabric. If there is a zone name conflict (the same zone name in each fabric) then the zones must have identical members for the fabrics to join. If the two zones have the same name but contain different members, then the E_Ports will segment and the fabrics will not join.

ATTENTION! If merging zones will result in segmented E_Ports and the fabrics will not join, you can join the fabrics by deactivating the active zone set on one of the fabrics (default zone is enabled). This eliminates any conflicts because the fabrics will then join using only the active zone set. After the fabrics join, you can make adjustments to zoning configurations.

Using The Zoning Page

Select *Configure* > *Zoning* on the navigation panel. The *Zoning* configuration page (Figure 4-3) displays. This page is used to configure zoning on the product. The page has three panels:

- *Potential Zone Members*—Used to add members to the zone. This consists of a listing of attached nodes and an interface for adding zone members by WWN or the combination of domain ID and port number.
- *Zone Name*—This panel is used to create and modify zones. The list of zone members shown in the *Pending Zone Members* area is pending in the sense that it is a work area; changes made in this area are not saved until the zone is added into a zone set.
- *Zone Set*—This panel is used to create and modify zone sets. Changes made in this panel are not made active in the fabric until they are activated using the *Activate* button.

Arrow buttons are used to move items between the panels. Zone members are added and deleted from the zone using the arrow buttons. Zones are added to the zone set using the arrow buttons.

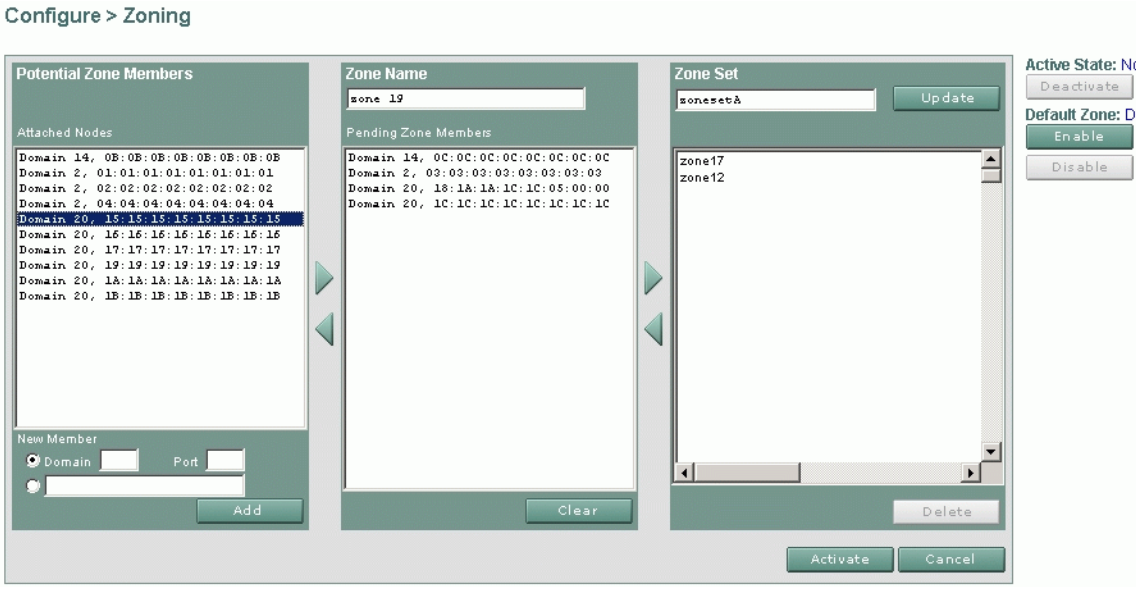


Figure 4-3 Zoning Page

Creating and Modifying a Zone

Perform this procedure to configure, add, or delete zones. A zone is a group of devices that can access each other through port- to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot. For a listing of limits on parameters regarding zones, see Table 4-1 on page 4-10.

ATTENTION! If, in your business practices, zoning tasks are performed using both the Command Line Interface (CLI) and the EFCM Basic interface, you risk conflicts in the configuration and functionality could be lost. It is recommended that they not be used simultaneously.

To configure zones, select *Configure* > *Zoning* on the navigation panel. The *Zoning* configuration page (Figure 4-3) displays.

Zones are created and modified in the *Zone Name* panel of the page. Potential zone members are added to the Pending Zone Members area, which shows the list of zone members.

You can use this panel to perform the following tasks:

- *Create a New Zone* on page 4-14
- *Add Zones Members to a Zone* on page 4-15
- *Remove Zone Members from a Zone* on page 4-16
- *Save the Zone to the Zone Set* on page 4-16
- *Rename a Zone* on page 4-16

Create a New Zone

The two primary attributes of a zone are the zone name and the list of zone members. To configure a zone, you can start with a blank zone or by using an existing zone.

First add the zone name in the *Zone Name* field. The following naming conventions apply to zones and zone sets:

- All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.
- The first character of a zone set name must be a letter (**A** through **Z** or **a** through **z**).

- A zone set name cannot contain spaces.
- Valid characters are alphanumerics and the caret (^), hyphen (-), underscore (_), or dollar ($) symbols.
- A zone set name can have a maximum of 64 characters.

NOTE: A product can have at most 1024 zones.

Add zone members as described in *Add Zones Members to a Zone* on page 4-15.

Add Zones Members to a Zone

Use the *Potential Zone Members* panel to add members to the zone. You can add members using the list of *Attached Nodes* or use the *New Member* dialog.

- *Attached Nodes*—You can use the arrow buttons between the panels to move selected nodes between this list and the *Pending Zone Members* list. You can select one item or multiple. This list is automatically populated at all times with the complete list of attached nodes.
- *New Members*—Add a new member either by the combination of domain ID and port number, or by WWN as follows:
  - Domain ID and port number—Select the radio button next to the *Domain* field. Put the domain ID in the *Domain* field and the port number in the *Port* field. Click the *Add* button to add the new zone member to the *Pending Zone Members* list.
  - WWN—Select the radio button next to the WWN field. Type the WWN of the new zone member in the field. Click the *Add* button to add the new zone member to the *Pending Zone Members* list.

NOTE: Changes to a zone or zoning configuration are not saved and activated on the product until saved as part of a zone set. See *Create a Zone Set* on page 4-17 for procedures.

Remove Zone Members from a Zone

Remove a member from the *Pending Zone Members* list using the arrow buttons between the panels. To delete all zone members, select the *Clear* button.

NOTE: If you use the arrow button to remove a zone member listed by WWN or the combination of domain ID and port number, the zone member is deleted from the *Pending Zone Members* list. It may not display in the *Attached Nodes* list unless the device is attached to the switch.

Save the Zone to the Zone Set

To save the zone, you add it to the zone set, using the arrow button to move it from the *Zone Name* panel to the *Zone Set* panel. The zone set is saved when you select the *Update* button.

Rename a Zone

To rename a zone, use the following procedure:

1. Select a zone in the *Zone Set* panel.
2. Use the arrow button to move the zone to the *Zone Name* panel.
3. Type a new zone name in the Zone Name field. (See the naming conventions described in *Create a New Zone* on page 4-14.)
4. Delete the old zone name by selecting the zone on the *Zone Set* panel and selecting the *Delete* button.
5. Add the renamed zone to the zone set using the arrow button to move it to the *Zone Set* panel.

Configuring the Zone Set

A zone set is a group of zones that is activated or deactivated as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time (although the default zone can be active at the same time as a zone set). For a listing of limits on parameters regarding zones, see Table 4-1 on page 4-10.

To configure zones sets, select *Configure* > *Zoning* on the navigation panel. The *Zoning* configuration page (Figure 4-3) displays.

Zone sets are created and modified in the *Zone Set* panel. You can use this panel to perform the following tasks:

- *Create a Zone Set* on page 4-17
- *Name and Rename a Zone Set* on page 4-18
- *Add Zones to the Zone Set* on page 4-18
- *Delete Zones From the Zone Set* on page 4-19
- *Change a Zone that is in the Zone Set* on page 4-19
- *Activate and Cancel the Zone Set Changes* on page 4-19
- *Deactivate the Active Zone Set* on page 4-20
- *State of the Default Zone* on page 4-20

Create a Zone Set

A zone set has two primary attributes, the zone set name and the list of zones that are members of the zone set. Both of these are configured using the *Zone Set* panel.

To set the zone set name, use the procedure described in *Name and Rename a Zone Set* on page 4-18.

To add zones to the zone set, use the procedures described in *Add Zones to the Zone Set* on page 4-18.

When you have defined all of the attributes of the zone set, click the *Update* button to save the configuration. The zone set is not active on the fabric until you select the *Activate* button. For information about activating and canceling changes, see *Activate and Cancel the Zone Set Changes* on page 4-19.

Name and Rename a Zone Set

Name or rename a zone set by typing in the *Zone Set* field and selecting the *Update* button. This changes the zone set name in the zone set work area and highlights the *Activate* button. Select the *Activate* button to distribute this change across the fabric.

NOTE: The zone set change is not active on the fabric until you select the *Activate* button. For more information, see *Activate and Cancel the Zone Set Changes* on page 4-19.

The following naming conventions apply to zone sets:

- All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.
- The first character of a zone set name must be a letter (**A** through **Z** or **a** through **z**).
- A zone set name cannot contain spaces.
- Valid characters are alphanumerics and the caret (**^**), hyphen (**-**), underscore (_), or dollar (**$**) symbols.
- A zone set name can have a maximum of 64 characters.

NOTE: A product can have at most 1024 zones.

Add Zones to the Zone Set

The *Zone Name* panel is used to create zones that are added to the Zone Set. The arrow buttons between the *Zone Name* and *Zone Set* panels are used to move zones between the panels.

Use the following procedure to add zones to the zone set:

1. Create a zone as described in *Create a New Zone* on page 4-14.
2. Use the arrow buttons between the panels to move the zone into the *Zone Set* panel.
3. Save the zone set by selecting the *Update* button. (The zone set is not active on the fabric until you select the *Activate* button.)

NOTE: The zone set change is not active on the fabric until you select the *Activate* button. For more information, see *Activate and Cancel the Zone Set Changes* on page 4-19.

Delete Zones From the Zone Set

Deleting a zone set deletes the zone from system memory. When a zone set is deleted, it is no longer available for configuration. Use the following procedure to delete zones from the zone set:

1. Select a zone listed in the *Zone Set* panel.
2. Select the *Delete* button.
3. Save the zone set changes by selecting the *Update* button. Once you select the *Update* button, the deletion of the zone cannot be canceled.

NOTE: The zone set change is not active on the fabric until you select the *Activate* button. For more information, see *Activate and Cancel the Zone Set Changes* on page 4-19.

Change a Zone that is in the Zone Set

The *Zone Name* panel is used to configure a zone. In order to make changes to a zone that is in the zone set, you must move the zone to the *Zone Name* panel. The arrow buttons between the *Zone Name* and *Zone Set* panels are used to move zones between the panels.

Use the following procedure to change a zone that is in the zone set:

1. Select a zone listed in the *Zone Set* panel.
2. Use the arrow buttons between the panels to move the zone into the *Zone Name* panel.
3. Make the desired changes to the zone as described in *Creating and Modifying a Zone* on page 4-14.
4. When you have completed changing the zone, use the arrow buttons between the panels to move the zone into the *Zone Set* panel.
5. Save the zone set by selecting the *Update* button.

NOTE: The zone set is not active on the fabric until you select the *Activate* button. For more information, see *Activate and Cancel the Zone Set Changes* on page 4-19.

Activate and Cancel the Zone Set Changes

Changes to zoning made on the *Zoning* page are not activated on the fabric until the *Activate* button is selected. The *Activate* button highlights whenever the zone set shown on the page is different from the zone set currently active on the fabric. Changes to the zone set are

not activated on the fabric until the user activates the changes. Instead, the changes remain local to the product.

Selecting the *Cancel* button clears all changes to the zone set. When the Cancel button is selected, the configuration dialogs show active zone set information.

Deactivate the Active Zone Set

The state of the zone set is shown in the *Active State* field. This field has the following values:

- *Active*—Indicates that a zone set is active in the fabric. (The active zone set may not be the same as the one shown in the *Zone Set* panel.)
- *Inactive*—Indicates that no zone set is active on the fabric.

When a zone set is active, the *Deactivate* button is enabled. Select the *Deactivate* button to make the zone set inactive. This action removes the current zone set from the *Fabric* and places all attached devices into the Default Zone.

State of the Default Zone

The state of the default zone is shown in the *Default Zone* field. This field has the following values:

- *Enabled*—Indicates that the default zone is enabled in the fabric. All devices and ports not configured as members of the active zone set are able to communicate.
- *Disabled*—Indicates that the default zone is disabled in the fabric. All devices and ports not configured as members of the active zone set cannot communicate.

When the default zone is enabled, select the *Disable* button to disable it. When the default zone is disabled, select the *Enable* button to enable it.

NOTE: Enabling the default zone while a zone set is active places all attached devices not currently in an active zone into the default zone.

5

Configuring Security

The *Security* menu is used to configure the ability of users and devices to communicate with the product. You must be logged in with administrator access to use the commands on the *Security* menu. The Security menu provides the following options:

- *Configuring User Authentication* 5-2
- *Configuring Software Authentication* 5-6
- *Configuring Device Authentication* 5-10
- *Configuring Port Authentication* 5-14
- *Configuring the IP Access Control List* 5-15
- *Configuring the RADIUS Server* 5-18
- *Enabling the Enterprise Fabric Mode* 5-22
- *Configuring Fabric Binding* 5-25
- *Configuring Switch Binding* 5-29
- *Configuring Port Binding* 5-33
- *Enabling and Disabling Safe Zoning Mode* 5-34
- *Upgrade Options* 5-35

Defining Authentication Settings

The *Authentication Settings* page allows the user to configure authentication parameters for Users, Software, Devices, and Ports.

The *Authentication Settings* page has tabs that are used to configure various types of authentications:

- Users tab—*Configuring User Authentication* on page 5-2
- Software tab—*Configuring Software Authentication* on page 5-6

- Devices tab—*Configuring Device Authentication* on page 5-10
- Ports tab—*Configuring Port Authentication* on page 5-14

Configuring User Authentication

The *User Authentication* configuration page (the default landing page when clicking on the *Authentication Settings* menu item) allows the EFCM Basic user to configure authentication settings for users of the product's embedded management interfaces, EFCM Basic and the CLI. This page configures all user names for EFCM Basic and the CLI.

The page has the following parts:

- *Existing Users*—A list of the user names currently configured for the product, which is documented in *Adding, Editing, and Deleting User Names* on page 5-2.
- *User Properties*—An interface used to configure the properties of the user name, which is documented in *Defining User Properties* on page 5-4.
- *Authentication Settings*—An interface used to configure the authentication settings used for the EFCM Basic (web) interface and the CLI, which is documented in *Defining Authentication Settings for the Product* on page 5-5.

Adding, Editing, and Deleting User Names

To add, edit and delete user names, use the *Existing Users* area of the *Users Authentication* page. Select *Security* > *Authentication Settings* on the navigation panel, then select the *Users* tab. The *Users Authentication* configuration page (Figure 5-1) displays.

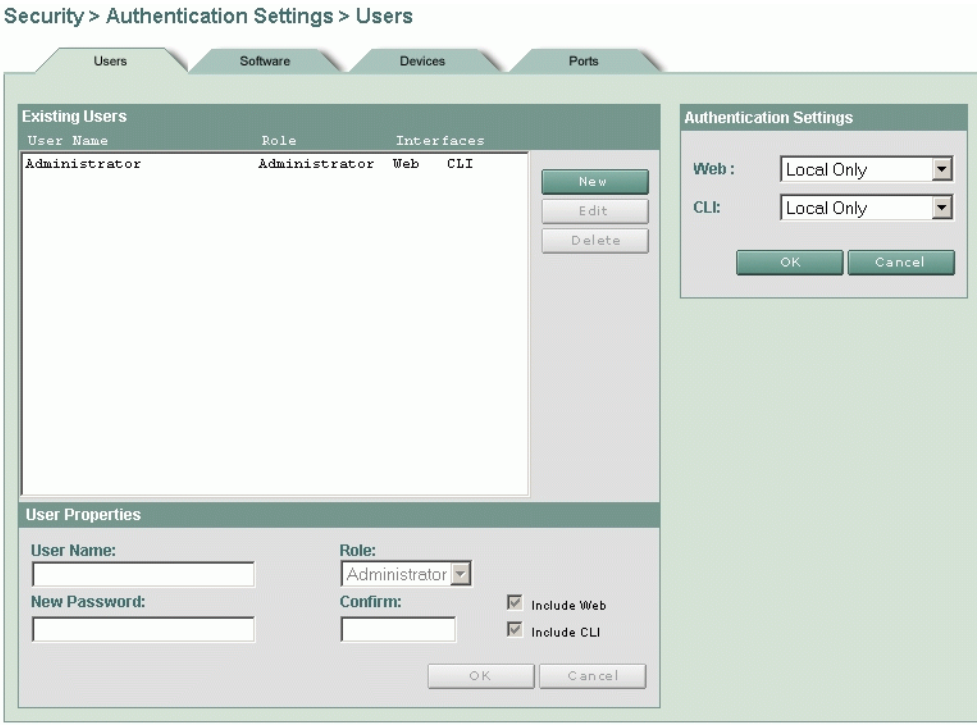


Figure 5-1 User Authentication Configuration Page

Use the page to perform the following tasks:

- Add a user name by selecting the *New* button. Use the *User Properties* area to configure settings for the user name as described in *Defining User Properties* on page 5-4.
- Edit a user name by selecting the user name from the list, then select the *Edit* button. Use the *User Properties* area to configure settings for the user name as described in *Defining User Properties* on page 5-4.
- Delete a user name by selecting the user name from the list, then select the *Delete* button.

NOTE: You cannot delete the last user name that is currently logged in with the role of Administrator and is making the authentication changes.

Defining User Properties

To configure the properties of user names, use the *User Properties* area of the *Users Authentication* page. Select *Security* > *Authentication Settings* on the navigation panel, then select the *Users* tab. The *Users Authentication* configuration page (Figure 5-1 on page 5-3) displays.

The *User Properties* area of the page becomes active when a user name is added or edited as described in *Adding, Editing, and Deleting User Names* on page 5-2.

The *User Properties* area allows the user to configure the following items:

- *User Name*—Specify a user name of up to 23 characters. Spaces, single quotes, double quotes, and colons are not allowed in the user name.
- *Role*—Specify the role for the user name from the drop-down list with selection of role-based privileges: Administrator, Operator, and No Role.

NOTE: If you assign the value No Role, this creates a user name that is not authorized to perform tasks but for which you can go back later to assign a role as either an Administrator or Operator. Therefore, if you want to create a user name and then later assign a role to the user name, you would initially select the No Role option.

- *New Password*—If a new password is desired, specify a password of up to 24 characters. If no new password is supplied, the password is unchanged.
- *Confirm*—Used to confirm the password text typed into the *New Password* text box. Retype the password in this box.
- *Include Web*—Select this check box to allow the user to log in using the web interface (EFCM Basic).
- *Include CLI* check box—Select this check box to allow the user to log in using the CLI.

Select the *OK* button to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.

Defining Authentication Settings for the Product

To configure how the product authenticates login attempts, use the *Authentication Settings* area of the *Users Authentication* page. Select *Security* > *Authentication Settings* on the navigation panel, then select the *Users* tab. The *Users Authentication* configuration page (Figure 5-1 on page 5-3) displays.

Use the drop-down menus to specify the authentication sequence used for web (EFCM Basic) and CLI logins. The following options are available for authenticating a user ID and its password:

- *Local Only*—only local authentication is performed. That is to say, authentication is performed by the product (local device) only.
- *RADIUS Only*—only the RADIUS server is used for authentication.
- *RADIUS then Local*—first the RADIUS server is used for authentication, then the local device.

Select the *OK* button to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.

User Accounts with RADIUS Server

When creating user accounts for a RADIUS server, you will need to compare McDATA user roles with RADIUS service type:

- McDATA Administrator is the same as a RADIUS Administrative service type.
- McDATA Operator is the same as a RADIUS Operator service type.

Configuring Software Authentication

The *Software Authentication* configuration page provides the ability to configure authentication settings for management access to the product. The management access configured by this page includes both in-band and out-of-band software access and settings for the API path (NMRU) and OSMS.

The *Software Authentication* configuration page has the following parts:

- Permitted Management Software list, which is described in *Defining Which Software Is Authenticated* on page 5-6.
- Software Member configuration dialog, which is described in *Configuring Software Authentication Properties* on page 5-8.
- Authentication Settings for API out-of-band access to the switch *Configuring Out-of-Band Settings* on page 5-8.
- OSMS Settings for in-band access to the switch *Configuring OSMS Settings* on page 5-9.

Defining Which Software Is Authenticated

To add, edit, and delete management software programs that are permitted to access the product, use the *Permitted Management Software* area of the *Users Authentication* page. Select *Security* >

Authentication Settings on the navigation panel, then select the *Software* tab. The *Software* configuration page (Figure 5-2) displays.

Figure 5-2 Software Authentication Configuration Page

The *Permitted Management Software* list shows authenticated out-of-band software identifiers (such as NMRU connections to the switch). Add, edit, and delete the software packages as follows:

- Add a software package by selecting the *New* button. Use the *Software Member* area to configure settings for the software as described in *Configuring Software Authentication Properties* on page 5-8.
- Edit a listed software package by selecting the software ID from the list, then selecting the *Edit* button. Use the *Software Member* area to configure settings for the software as described in *Configuring Software Authentication Properties* on page 5-8.
- Delete a software package by selecting the software ID from the list, then selecting the *Delete* button. To delete all listed software, select the *Delete All* button.

Configuring Software Authentication Properties

To configure the properties of a software ID, use the *Software Member* area of the *Users Authentication* page. Select *Security* > *Authentication Settings* on the navigation panel, then select the *Software* tab. The *Software* configuration page (Figure 5-2) displays.

The *Software Member* area becomes active when you add or edit a software ID as described in *Defining Which Software Is Authenticated* on page 5-6.

The *Software Member* area allows the user to configure the following items:

- *Software ID*—Specify a software ID of up to 23 characters. This should be the ID used by the software to log in. Spaces, single quotes, double quotes, and colons are not allowed in the ID.
- *CHAP Secret*—Specify the CHAP secret to be used by the software package during login. The secret must contain 16 characters (16 bytes).
- *Confirm Secret*—Enter the CHAP secret again to confirm it.

Select the *OK* button to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.

Configuring Out-of-Band Settings

The *Authentication Settings* area of the *Software* tab provides authentication configuration to secure access to the product from out-of-band software. It contains configuration for enabling and disabling software authentication, as well as setting the Authentication Sequence.

To configure how the product authenticates login attempts, use the *Authentication Settings* area of the *Software* tab of the *Authentication* page. Select *Security* > *Authentication Settings* on the navigation panel, then select the *Software* tab. The *Software* configuration page (Figure 5-2 on page 5-7) displays.

Use the drop-down menus to specify the authentication sequence used for software logins. The following options are available for authenticating a software ID and its password:

- *Authentication Sequence*—Use the drop-down menu to specify the authentication sequence used for out-of-band software. The following options are available for authenticating a software ID and its CHAP secret:

  - — *Local Only*—Only local authentication is performed. That is to say, authentication is performed by the product (local device) only.
  - — *RADIUS Only*—Only the RADIUS server is used for authentication.
  - — *RADIUS then Local*—First the RADIUS server is used for authentication, then the local device.
- *Outgoing Authentication*—Specify whether outgoing authentication is enabled or disabled. From the drop-down list, select *Enabled* to enable outgoing authentication and *Disabled*, to disable it.

Select the *OK* button to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.

Configuring OSMS Settings

The *OSMS* area of the *Software* tab provides authentication configuration to secure access to the product from the Open Systems Management Server (OSMS). It contains configuration for enabling and disabling software authentication, as well as setting the Authentication Sequence

To configure how the product authenticates OSMS login attempts, use the *OSMS Settings* area of the *Software* tab of the *Authentication* page. Select *Security* > *Authentication Settings* on the navigation panel, then select the *Software* tab. The *Software* configuration page (Figure 5-2 on page 5-7) displays.

Use the fields of this area to configure OSMS login attempts:

- *Outgoing Authentication*—Specify whether outgoing authentication is enabled or disabled. From the drop-down list, select *Enabled* to enable outgoing authentication and *Disabled*, to disable it.
- *Authentication Key*—Specify the machine-generated Authentication Key. The key must be 16 characters (16 bytes).
- *Confirm Key*—Enter the authentication key value again to confirm it.

Select the *OK* button to save and activate the changes. The message **Your changes have been successfully activated** displays below the page's heading.

Configuring Device Authentication

The *Device Authentication* page allows the user to configure authentication for both attached and detached devices. This page specifies whether the product authenticates requests from other devices for connection.

Select *Security* > *Authentication Settings* on the navigation panel, then select the *Device* tab. The *Device Authentication* configuration page (Figure 5-3) displays.

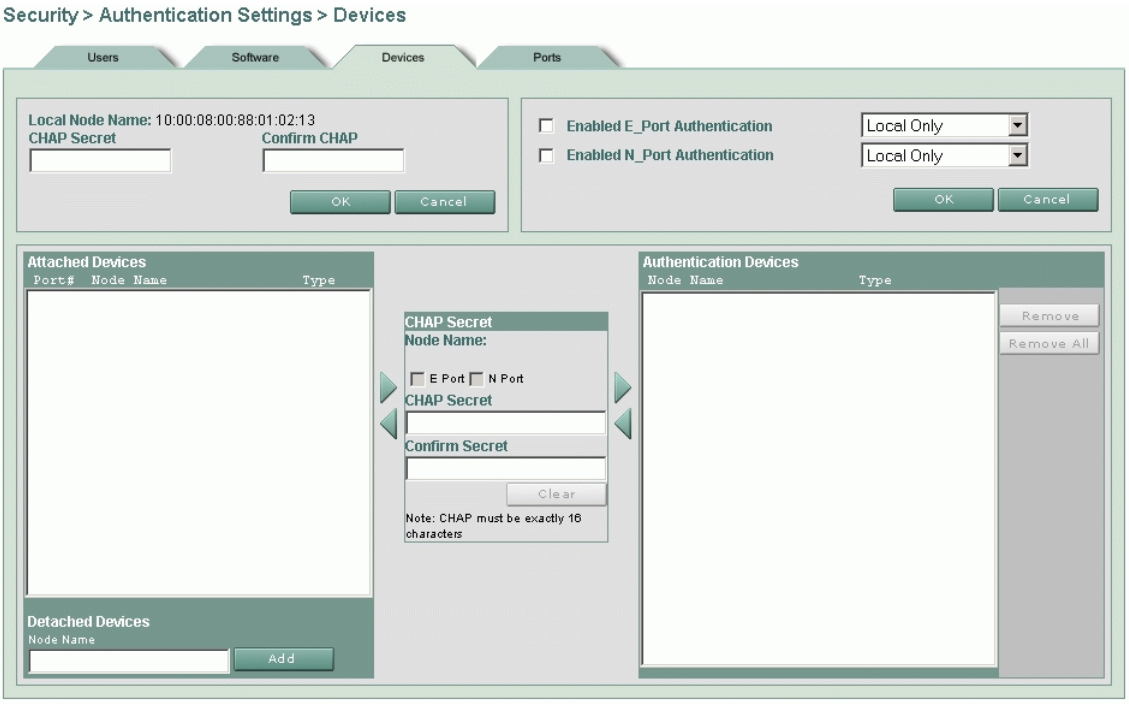


Figure 5-3 Device Authentication Configuration Page

The page consists of the following parts:

- Dialog for setting the CHAP secret for the product, which is described in *Defining the CHAP Secret of the Product* on page 5-11.
- Dialog for setting the port authentication sequence for E_Ports and N_Ports, which is described in *Defining Port Authentication Sequences* on page 5-11.

- Dialog for adding devices to the list of Authenticated Devices. These devices are allowed to make connections to the product, which is described in *Configuring Authentication Devices* on page 5-12.

Defining the CHAP Secret of the Product

The top left of the *Device Authentication* page contains a dialog for defining the CHAP secret of the product. The WWN of the product displays in the *Local Node Name* field.

To specify a CHAP secret for the product, enter a 16-character CHAP secret in the *CHAP Secret* field. Enter the same sequence of characters in the *Confirm CHAP* field.

Select the *OK* button to save and activate the CHAP secret.

Defining Port Authentication Sequences

You can configure the port authentication sequences to be used by the product's E_Ports and N_Ports. The user has the option of selecting authentication parameters for E Ports and N Ports at the top right of the page. It allows the user to configure the Authentication Sequence (RADIUS, then Local; RADIUS only; or Local only) that specifies the way of authenticating the E/N port devices. Selecting the *OK* button sends the contents to the switch, while selecting the *Cancel* button reloads the dialog with current switch settings.

- Enable authentication—select the *Enabled E_Port Authentication* check box to enable authentication on E_Ports. Select the *Enabled N_Port Authentication* check box to enable authentication on N_Ports. Clear the appropriate check box to disable port authentication.
- Authentication Sequence—Use the drop-down menu to specify the authentication sequence used for out-of-band software. The following options are available for authenticating a software ID and its CHAP secret:
  - — *Local Only*—Only local authentication is performed. That is to say, authentication is performed by the product (local device) only.
  - — *RADIUS Only*—Only the RADIUS server is used for authentication.
  - — *RADIUS then Local*—First the RADIUS server is used for authentication, then the local device.

Select the *OK* button to save the settings. You can select *Cancel* to load the dialog with the product's currently active values.

Configuring Authentication Devices

The lower part of the *Device Authentication* page is used to configure authentication for remote devices. This part of the screen has the following components:

- *Attached Devices* list and *Detached Devices* dialog—Used to specify the devices for which you are configuring authentication.
- *CHAP Secret* dialog—Used to configure the CHAP secret to be used by the device.
- *Authentication Devices* dialog—A list of the nodes for which authentication is configured, used to add and remove devices from the Authentication Devices list.

Selecting Devices to be Authenticated

In order to be added to the Authentication Devices list, a device must have a CHAP secret specified for it in the *CHAP Secret* dialog. Devices are added to the *CHAP Secret* dialog as follows:

- Select a device from the *Attached Devices* list. The list is a selectable (single-select only) list of WWNs of all devices that are attached to the product. Use the arrow button to move the device to the *CHAP Secret* dialog.
- Specify a detached device in the *Detached Devices* dialog. Enter a valid WWN in the *Node Name* field. Select the *Add* button to move the device to the *CHAP Secret* dialog.

Applying a CHAP Secret to the Device

When the *CHAP Secret* dialog has been populated, the WWN of the device will be seen at the top of the dialog in un-editable text.

To specify a CHAP secret for the device, enter a 16-character CHAP secret in the *CHAP Secret* field. Enter the same sequence of characters in the *Confirm Secret* field.

Specify whether the device is an E_Port or an N_Port by selecting the *E_Port* check box or the *N_Port* check box.

You can select the *Clear* button to clear the dialog of the shown values.

You can use the arrow buttons between the *CHAP Secret* and *Authentication Devices* areas to add the device to the Authentication Devices list. For more information, see *Adding a Device to the Authentication Devices List* on page 5-13.

If you use the arrow buttons between the *Attached Devices* and *CHAP Secret* panels to return the device to the *Attached Devices* panel, no CHAP secret value is assigned to the device. If the device is a detached device, the WWN of the device is removed.

Adding a Device to the Authentication Devices List

The arrow buttons between the *Chap Secrets* dialog and the *Authentication Devices* dialog are used to add and remove devices from the Authentication Devices list.

NOTE: The number of the E_Port and N_Port device records is limited to 768 records for 12-Port Switch, 24-Port Switch, 16-Port 4-Gbps Switch, and 32-Port 4-Gbps Switch. The limit is 252 records for the 140-Port Director. The limit is 128 records for the 16-Port 2-Gbps Switch, 32-Port 2-Gbps Switch, and 64-Port Director.

In order to add a device to the Authentication Devices list, you must complete the fields of the CHAP Secret dialog as described in *Applying a CHAP Secret to the Device* on page 5-12. Use the arrow button between the *CHAP Secret* and *Authentication Devices* areas to add the device to the Authentication Devices list. The device is configured to be authenticated immediately after being added to the list.

The Authenticated Devices list shows the WWN and type of each device on the list. You can select the devices individually and send back the *CHAP Secret* dialog for editing using the arrow button. This does not remove the device from the list.

Removing a Device from the Authentication Devices List

Remove a device from the Authentication Device list by selecting it, then selecting the *Remove* button. This removes the CHAP secret configuration from the device.

Attached devices that are removed from the list are re-populated to the *Attached Devices* dialog. Detached devices that are removed are permanently deleted from the page.

Configuring Port Authentication

The *Port Authentication* page allows a user to override the authentication settings of the product for specified ports. The page shows a list of ports, their WWN (if applicable), and their authentication state.

To configure authentication for a port, perform the following procedures:

1. Select *Security* > *Authentication Settings* on the navigation panel, then select the *Port* tab. The *Port Authentication* configuration page (Figure 5-4) displays.

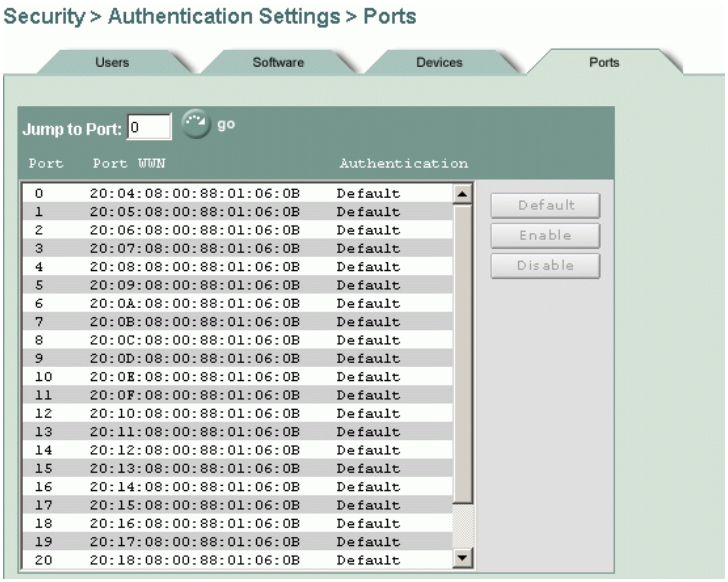


Figure 5-4 Port Authentication Configuration Page

2. Select the port or ports for which you will change authentication configuration.
3. Specify the authentication state for the port by selecting one of the following buttons:
   - *Default*—Specifies that the port use the authentication setting that is active for the product.
   - *Enable*—Specifies that authentication is enabled for the port.

- *Disable*—Specifies that authentication is disabled for the port.

The changes are immediately applied to the port and the list is updated with the new information.

Configuring the IP Access Control List

The *IP Access Control List* page enables you to configure a list of trusted switch IP addresses that are allowed to make IP connections to the product. This list is called the IP Access Control List (IP ACL).

Select *Security* > *IP Access Control List* on the navigation panel. The *IP Access Control List* page (Figure 5-5) displays.

Figure 5-5 IP Access Control List

The display panel is divided into three sections:

- Switch IP Access Control List state dialog—Used to enable and disable IP ACL, which is described in *Setting the IP ACL State* on page 5-16.

- Switch IP Access Control List—A table containing all addresses configured as having access to the switch. This area is also used to delete members from the list, which is described in *Deleting Members from the List* on page 5-17.
- Add/Edit Members dialog—Used to add and edit entries for the list, which is described in *Adding New Members to the List* on page 5-16 and *Editing the List* on page 5-17.

Setting the IP ACL State

The *IP Access Control List* field shows the enabled state of IP ACL. The values shown in this field are:

- Enabled—Indicates that IP ACL is enabled.
- Disabled—Indicates that IP ACL is disabled.

To enable IP ACL, select the *Enable* button. To disable IP ACL, select the *Disable* button.

NOTE: The Host IP address is the IP address of the management client, the computer used to run the EFCM Basic web browser. The Host IP address must be included in the IP ACL, or, as soon as the IP ACL is enabled, the management client will not be able to communicate with the switch.

Adding New Members to the List

To add new members to the *Switch IP Access Control List*, you can specify one IP address or a range of IP addresses in the *Add/Edit Members* dialog. You can configure a maximum of 32 entries on the list.

NOTE: The Host IP address is the IP address of the management client, the computer used to run the EFCM Basic web browser. The Host IP address must be included in the IP ACL, or, as soon as the IP ACL is enabled, the management client will not be able to communicate with the switch.

Add new members to the list as follows:

- *Single IP*—Specify the IP address to be added to the list in this field. Select the *OK* button to add the entry to the list.
- Range of IP addresses—To specify a range of IP addresses, type the first IP address in the range in the *Starting IP* field. Type the last IP address in the range in the *Ending IP* field. Select the *OK* button to add the range to the list.

Editing the List

Use the edit functionality of the *Switch IP Access Control List* to remove an entry from the list and replace with an updated entry. Edit an entry by selecting an entry on the *Switch IP Access Control List* and selecting the Edit button. The selected entry is populated to the *Add/Edit Members* dialog. Specify a new entry as described in *Adding New Members to the List* on page 5-16.

Deleting Members from the List

Delete members from the *Switch IP Access Control List* using the *Delete* and *Delete All* buttons.

NOTE: If the host IP address is selected or included in the selected range, deletion may cause EFCM Basic to become inaccessible.

To delete a single IP address or a range, select the desired item from the list. Select the *Delete* button. The deletion takes effect immediately on the fabric.

Or you can delete the entire list, by selecting the *Delete All* button. The change takes effect immediately on the fabric.

Configuring the RADIUS Server

The product has a RADIUS client that can access up to three user-configurable RADIUS servers. The *RADIUS Server* page enables you to configure a list of RADIUS servers that are used by the product for authentication.

NOTE: A RADIUS server is used to provide remote authentication and accounting. This document does not describe how to install a RADIUS server; additional information about RADIUS servers is provided with the product's documentation. For EFCM Basic, you will need to know some information such as how user accounts are created for a RADIUS server. Review *User Accounts with RADIUS Server* on page 5-5 for information on setting up user accounts which require data that is unique to the McDATA EFCM Basic interface.

Select *Security* > *RADIUS* on the navigation panel. The *RADIUS Server* page (Figure 5-6) displays.

The RADIUS Server list is shown in the *Radius Server* area of the page. The entries are shown in order of priority. The first entry has the highest priority; the second entry is next. Priority corresponds to the order in which the product uses the server for authentication. The highest priority entry is contacted first during a login attempt. If that server is unavailable, the next highest priority server is contacted.

Use this page to perform the following tasks:

- Add an entry to the RADIUS Server list for the product, which is described in *Add an Entry to the RADIUS Server List* on page 5-19.
- Edit information for a RADIUS Server, which is described in *Edit an Entry on the RADIUS Server List* on page 5-20.
- Delete an entry from the RADIUS Server list, which is described in *Delete an Entry from the RADIUS Server List* on page 5-20.
- Set the priority of the RADIUS Servers, which is described in *Configure Priority of the RADIUS Servers* on page 5-20.
- Set the Dead Time parameter for an unresponsive RADIUS Server, which is described in *Configure Priority of the RADIUS Servers* on page 5-20.

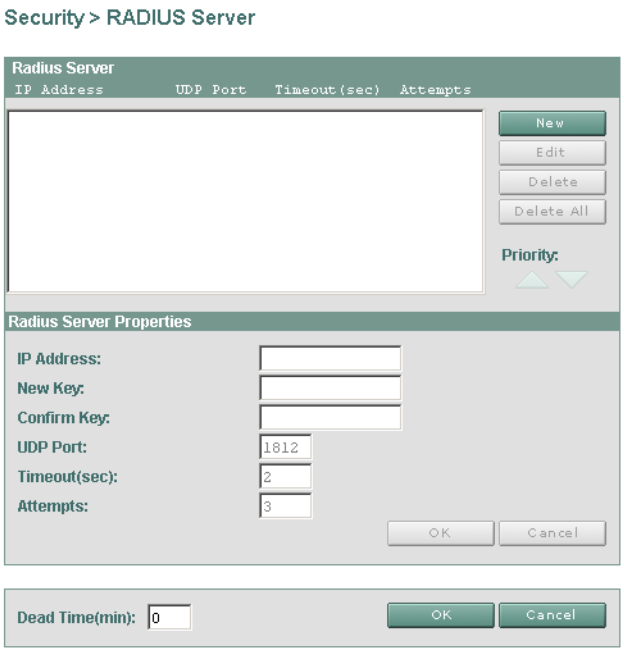


Figure 5-6 RADIUS Server Page

Add an Entry to the RADIUS Server List

The RADIUS Server list shows the RADIUS Servers the product is configured to use for authentication. The RADIUS Server list can have a maximum of three entries.

To create an entry in the RADIUS Server list, select the *New* button. The *Radius Server Properties* area becomes active. Specify values for the parameters in this area as follows:

- *IP Address*—Specify an IP address for the RADIUS Server.
- *New Key*—Enter a key that is consistent with the key on the RADIUS server. This can be a key of 1 to 255 characters in length.
- *Confirm Key*—Enter the value entered in the *New Key* field.
- *UDP Port*—Specify a UDP Port number. The default port number is 1812.

- *Timeout (sec)*—Specify the amount of time to wait for a response from the RADIUS server before re-transmitting information. The time-out value can be in the range 1 to 1000 seconds; the default is 4 seconds.
- *Attempts*—Specify the number of times an access-request packet is resent to a RADIUS server if a response is not received before the time-out. After the attempts limit is reached, the Gateway switches to the next server. The value can be 1 to 100 attempts; default is 3 attempts.

Select the *OK* button to add the entry to the RADIUS Server list.

Edit an Entry on the RADIUS Server List

To edit the configuration information for an entry in the RADIUS Server list, select an entry from the list in the *Radius Server* area of the *RADIUS Server* page. Select the *Edit* button. The information for the RADIUS Server is shown in the *Radius Server Properties* area of the page.

You can change values of the parameters for the RADIUS Server as described in *Add an Entry to the RADIUS Server List* on page 5-19.

Select the *OK* button to populate your changes to the RADIUS Server list.

Delete an Entry from the RADIUS Server List

To remove a RADIUS Server from the database, select the RADIUS Server from the list and select the *Delete* button. When deleting an entry from the list, the remaining servers in the list are moved to a higher priority.

To remove all RADIUS Servers from the list, select the *Delete All* button.

Configure Priority of the RADIUS Servers

Entries in the *Radius Server* part of the page are shown in order of priority. The first entry has the highest priority; the second entry is next. Priority corresponds to the order in which the product uses the server for authentication. The highest priority entry is contacted first during a login attempt. If that server is unavailable, the next highest priority server is contacted.

To change the priority of entries in the RADIUS Server list, select an entry from the list in the *Radius Server* area of the *RADIUS Server* page. Use the arrow buttons to raise or lower the priority of the selected entry.

Configuring the Dead Time Parameter

If a RADIUS server does not respond to an authentication request, it can be marked as dead (unavailable) for a specified time interval. During that time period the alternate, lower-priority server is used for authentication. This time interval is called "Dead Time" and is configured using the *Dead Time (min)* field at the bottom of the *RADIUS Server* page.

Identifying a server as unavailable may speed up authentication by eliminating time-outs and retransmissions. If no alternate RADIUS Servers are available (when only one server is configured or when all are marked dead or unavailable), the Dead Time value is ignored.

Specify the number of minutes an unavailable server should be bypassed for authentication in the *Dead Time (min)* field. Valid values for this parameter are integers in the range 0 to 1440 minutes. The default value is 0.

Enabling the Enterprise Fabric Mode

The *Enterprise Fabric Mode* page provides the ability to enable and disable the Enterprise Fabric Mode. The Enterprise Fabric Mode automatically enables the features that FICON devices need to participate in a fabric. These features are described in *Features and Parameters Enabled with Enterprise Fabric Mode* on page 5-22.

Select *Security* > *Enterprise Fabric Mode* on the navigation panel. The *Enterprise Fabric Mode* page (Figure 5-7) displays.

Figure 5-7 Enterprise Fabric Mode Page

Using this page, you can enable or disable the Enterprise Fabric Mode on the product. If the Enterprise Fabric Mode field displays *Disabled*, selecting the *Enable* will enable the mode. If the field displays *Enabled*, selecting the *Disable* button will disable the mode.

The function of Enterprise Fabric Mode depends on Fabric Binding and Switch Binding features that are enabled by the SANtegrity Binding licensed feature. To enable Enterprise Fabric Mode, the SANtegrity Binding feature has to be installed on all the products in the fabric.

Features and Parameters Enabled with Enterprise Fabric Mode

The features that are automatically enabled when Enterprise Fabric Mode is enabled are described in the following sections:

- *Fabric Binding and the Enterprise Fabric Mode* on page 5-23
- *Switch Binding and the Enterprise Fabric Mode* on page 5-23
- *Rerouting Delay and the Enterprise Fabric Mode* on page 5-23
- *Domain RSCNs and the Enterprise Fabric Mode* on page 5-24
- *Insistent Domain Identification (ID) and the Enterprise Fabric Mode* on page 5-24

Fabric Binding and the Enterprise Fabric Mode

Fabric Binding is a SANtegrity Binding feature that prohibits switches and directors from communicating with switches or directors that are not part of the fabric. Refer to *Configuring Fabric Binding* on page 5-25 for details on configuring Fabric Binding.

When the Enterprise Fabric Mode is enabled, Fabric Binding is enabled automatically. The fabric members that are currently attached to the product are added automatically to the active Fabric Binding Member List (active FBML), a list of switches and directors that are allowed to communicate with the product. Therefore, when Enterprise Fabric Mode is enabled, the fabric members that are currently attached to the product participate in Fabric Binding. To add other fabrics to the active FBML, see *Add Members to the FBML* on page 5-27.

Switch Binding and the Enterprise Fabric Mode

Switch Binding is a SANtegrity Binding feature that enables switches or directors to communicate only with devices that are listed on the Switch Binding Membership List (SBML). When the Enterprise Fabric Mode is enabled, Switch Binding is also enabled. You need to configure the SBML, which specifies the devices with which the switch or director can communicate. Refer to *Configuring Switch Binding* on page 5-29 for details on configuring Switch Binding.

Rerouting Delay and the Enterprise Fabric Mode

Rerouting Delay ensures that frames are delivered through the fabric to their destination in the correct order, even if the path changes. If traffic to a particular destination is going to be rerouted over a shorter path, the rerouting delay function prevents new traffic from being released before the existing traffic arrives at its destination.

If a change to the fabric topology creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This situation could result in frames being delivered to a destination out of order because frames sent over a new, shorter path may arrive before frames sent previously using the older, longer path.

If Rerouting Delay is enabled, traffic ceases in the fabric for the time specified in the *E_D_TOV* field of the *Fabric Parameters* configuration page (for more information, see *Configuring Fabric Parameters for the Switch* on page 3-14). This delay enables frames sent using the old path to arrive at their destination before frames begin traversing the new path.

If Enterprise Fabric Mode is enabled, Rerouting Delay is automatically enabled and cannot be disabled unless the director or

switch is offline. In this case, disabling Rerouting Delay also disables Enterprise Fabric Mode. For information about configuring and enabling Rerouting Delay, see *Configuring Switch Parameters* on page 3-11.

Domain RSCNs and the Enterprise Fabric Mode

Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

If Enterprise Fabric Mode is enabled, Domain RSCNs are automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Domain RSCNs also disables Enterprise Fabric Mode. For information about enabling Domain RSCNs, see *Configuring Switch Parameters* on page 3-11.

Insistent Domain Identification (ID) and the Enterprise Fabric Mode

If enabled, Insistent Domain ID specifies that the preferred domain ID configured for the product will be the product's active domain identification when the fabric initializes. For information about configuring the preferred domain ID, see *Configuring Switch Parameters* on page 3-11.

A static and unique domain ID is required by the Fabric Binding feature because the feature's FBML identifies switches by WWN and domain ID. If a duplicate preferred domain ID is used, then made insistent, warnings display when directors and switches are added to an FBML.

If Fabric Binding or Enterprise Fabric Mode is enabled, Insistent Domain ID is automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Insistent Domain ID disables Enterprise Fabric Mode and Fabric Binding. For information about configuring the domain ID and Insistent Domain ID, see *Configuring Switch Parameters* on page 3-11.

Configuring Fabric Binding

Fabric Binding functionality, provided by the SANtegrity Binding feature, allows you to bind the product to specified fabrics so that it can communicate only with those fabrics. With Fabric Binding enabled, the product can communicate only with fabrics that are included in the Fabric Binding Member List (FBML).

Using Fabric Binding, you can allow specific products to attach to specific fabrics in the SAN. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

The *Fabric Binding* page allows the user to modify Fabric Binding configuration, to save and activate any changes that have been made to Fabric Binding configuration, and to deactivate Fabric Binding. Fabric Binding is available only if the SANtegrity Binding feature is installed.

A number of settings must be configured correctly on the product for Fabric Binding to function. For a description of these, see *Enable, Disable, and Online State Functions* on page 5-26.

To configure Fabric Binding, select *Security* > *Fabric Binding* on the navigation panel. The *Fabric Binding* page (Figure 5-8) displays showing the current FBML. Use this page to perform the following tasks:

- Determine Fabric Binding status, which is described in *Identify Fabric Binding Status* on page 5-27.
- Load members of the current fabric to the FBML, which is described in *Load the Current Fabric to the FBML* on page 5-27.
- Add members to the FBML, which is described in *Add Members to the FBML* on page 5-27.
- Delete members from the FBML, which is described in *Delete Members from the FBML* on page 5-27.
- Activate Fabric Binding, which is described in *Activate Fabric Binding* on page 5-28.
- Deactivate Fabric Binding, which is described in *Deactivate Fabric Binding* on page 5-28.

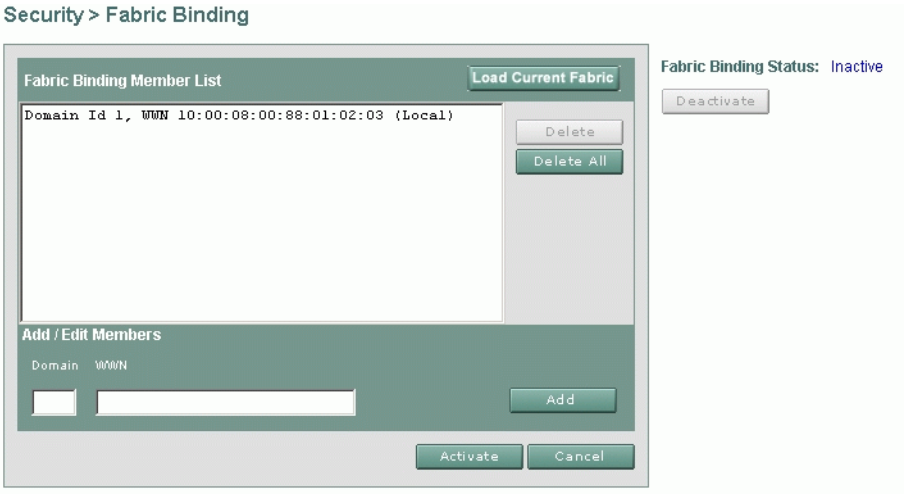


Figure 5-8 Fabric Binding Page

Enable, Disable, and Online State Functions

In order for Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Because switches are bound to a fabric by WWN and domain ID, the Insistent Domain ID function is automatically enabled if Fabric Binding is enabled. You cannot disable Insistent Domain ID while Fabric Binding is active and the switch is online. (For information about configuring the domain ID of the product, see *Configuring Switch Parameters* on page 3-11.)
- If Fabric Binding is enabled and the switch is online, you cannot disable Insistent Domain ID.
- If Fabric Binding is enabled and the director or switch is offline, you can disable Insistent Domain ID, but this will disable Fabric Binding.
- You cannot disable Fabric Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, Fabric Binding can be enabled or disabled.

Identify Fabric Binding Status

The *Fabric Binding* page provides the status of Fabric Binding for the product in the *Fabric Binding Status* field. The following values are shown in the field:

- *Active*—Fabric Binding is active on the fabric, which means that product can communicate only with the members of the FBML.
- *Inactive*—Fabric Binding is inactive, which means that Fabric Binding is disabled. The product can communicate with devices not in the fabric.

You can determine whether the *Fabric Binding Member List* shown in the page differs from the list of devices that are attached to the fabric. In this case, the *Activate* button is enabled, because FBML changes are pending. For more information about this, see *Activate Fabric Binding* on page 5-28.

Load the Current Fabric to the FBML

If you want, you can load members of the current fabric to the *Fabric Binding Member List*. Select the *Load Current Fabric* button to populate the *Fabric Binding Member List* shown on *Fabric Binding* page.

The FBML list shown in the page is not active on the fabric until the FBML is activated. For more information, see *Activate Fabric Binding* on page 5-28.

Add Members to the FBML

Use the *Add/Edit Members* dialog of the *Fabric Binding* page to add a new member to the *Fabric Binding Member List*. Type the domain ID of the device you want to add to the list in the *Domain* field. Type the WWN of the device in the *WWN* field. Select the Add button to add the device as a new member of the *Fabric Binding Member List*.

NOTE: The FBML can contain a maximum of 239 members.

The FBML list shown in the page is not active on the fabric until the changes are activated. For more information, see *Activate Fabric Binding* on page 5-28.

Delete Members from the FBML

To delete an entry from the *Fabric Binding Member List*, select the entry. Select the *Delete* button to delete the member. To completely clear the list of members, select the *Delete All* button.

NOTE: If Fabric Binding is active, you cannot delete members from the list that are attached to the fabric. Members that are attached must remain in the list, because the list must contain all attached members to be activated.

The FBML list shown in the page is not active on the fabric until the changes are activated. For more information, see *Activate Fabric Binding* on page 5-28.

Activate Fabric Binding

Selecting the *Activate* button of the Fabric Binding page results in the following activities:

- The entries shown in the *Fabric Binding Member List* are saved as the active FBML.
- Fabric Binding is activated for the product

NOTE: Fabric Binding is also enabled automatically, when the Enterprise Fabric Mode is enabled. However, in this case, only attached fabric members are included in the active FBML. For more information, see *Fabric Binding and the Enterprise Fabric Mode* on page 5-23.

The Activate button is enabled only when the *Fabric Binding Member List* is different from the FBML that is saved. If Fabric Binding status is inactive, load the currently attached devices to the *Fabric Binding Member List* (see *Load the Current Fabric to the FBML* on page 5-27) to enable the *Activate* button.

Deactivate Fabric Binding

Selecting the *Deactivate* button to change the Fabric Binding status from active to inactive, disabling Fabric Binding.

NOTE: You cannot deactivate Fabric Binding if Enterprise Fabric Mode is enabled.

Configuring Switch Binding

Switch Binding functionality enables you to identify the devices with which the switch or director can communicate. Switch Binding is available only if the SANtegrity Binding feature is installed.

The *Switch Binding* page allows you to enable the product to communicate only with devices that are listed on the Switch Binding Membership List (SBML). Switch Binding restricts connections to only the devices listed on the SBML and allows no other devices to communicate with the switch. When an unauthorized WWN attempts to log in, it is denied a connection and an event is posted to the event log. This provides security in environments that include a large number of devices by ensuring that only the specified set of devices is able to attach to a switch or director.

You can use the *Switch Binding* page to enable Switch Binding and to create and change the SBML.

NOTE: Switch Binding can also be enabled by enabling the Enterprise Fabric Mode. For more information, see *Switch Binding and the Enterprise Fabric Mode* on page 5-23.

To configure Switch Binding, select *Security* > *Switch Binding* on the navigation panel. The *Switch Binding* page (Figure 5-9) displays showing the current SBML. Use this page to perform the following tasks:

- Set the state of Switch Binding, which is described in *Define Switch Binding State* on page 5-31.
- Add members to the SBML, which is described in *Adding Members to the SBML* on page 5-31.
- Remove members from the SBML, which is described in *Removing Members from the SBML* on page 5-32.

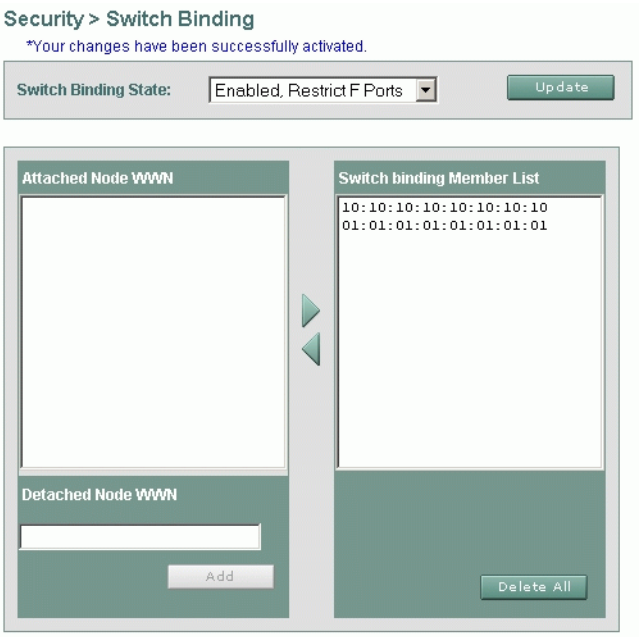


Figure 5-9 Switch Binding Page

Enable, Disable and Online State Functions

For Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features:

- Switch Binding can be enabled or disabled whether the product is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Switch Binding.
- If Enterprise Fabric Mode is enabled and the director or switch is online, you cannot disable Switch Binding.

- If Enterprise Fabric Mode is enabled and the director or switch is offline you can disable Switch Binding, but this also disables Enterprise Fabric Mode.
- WWNs can be added to the SBML without regard to whether Switch Binding is enabled or disabled.
- If the director or switch is online and Switch Binding is not enabled, all nodes and switches attached to the director or switch are automatically added to the SBML.

Define Switch Binding State

NOTE: Switch Binding can also be enabled by enabling the Enterprise Fabric Mode. For more information, see *Switch Binding and the Enterprise Fabric Mode* on page 5-23.

Enable or disable Switch Binding by selecting one of the following options from the *Switch Binding State* drop-down list. Available selections are:

- *Enabled, Restrict E Ports*—Enables the switch to bind to devices listed on the SBML through E_Ports only.
- *Enabled, Restrict F Ports*—Enables the switch to bind to devices listed on the SBML through F_Ports only.
- *Enabled, Restrict All Ports*—Enables the switch to bind to devices listed on the SBML through all port types.
- *Disabled*—Sets the Switch Binding State to disabled. No restrictions apply as to which devices can attach to this switch. This option is not valid if Enterprise Fabric Mode is enabled.

Select the *Update* button to activate your choice.

Adding Members to the SBML

NOTE: The SBML can contain a maximum of 256 WWN entries.

In the Switch Binding page, you add both attached nodes and detached nodes to the SBML. Use the following procedures to add members to the SBML:

- Attached nodes—The Attached Node WWN field is automatically populated with the WWNs of all nodes that are attached to the fabric. Use the arrow button between the *Attached Node WWN* panel and the *Switch Binding Member List* panel to add the selected WWN to the *Switch Binding Member List*. (The maximum number of attached nodes that can be shown is less

than 256 for some products. The limit is 252 for the 140-Port Director. The limit is 128 for the 16-Port 2-Gbps Switch, 32-Port 2-Gbps Switch, and 64-Port Director.)

- Detached nodes—Enter the WWN of a detached node in the *Detached Node WWN* field. Select the Add button to add the WWN to the *Switch Binding Member List*.

Removing Members from the SBML

To delete a WWN from the SBML, select the WWN from the *Switch Binding Member List*. Use the arrow button between the *Attached Node WWN* panel and the *Switch Binding Member List* panel to remove the WWN from the SBML. If the WWN is for an attached node, it is added to the *Attached Node WWN* panel. If the WWN is for a detached node, the WWN is removed from system memory.

To delete all members of the *Switch Binding Member List*, select the *Delete All* button. Attached nodes are returned to the *Attached Node WWN* panel, and detached nodes are deleted from system memory.

Configuring Port Binding

The *Port Binding* page enables you to bind a specific switch or director port to the WWN of an attached device for exclusive communication.

To configure Port Binding, select *Security* > *Port Binding* on the navigation panel. The *Port Binding* page (Figure 5-10) displays.

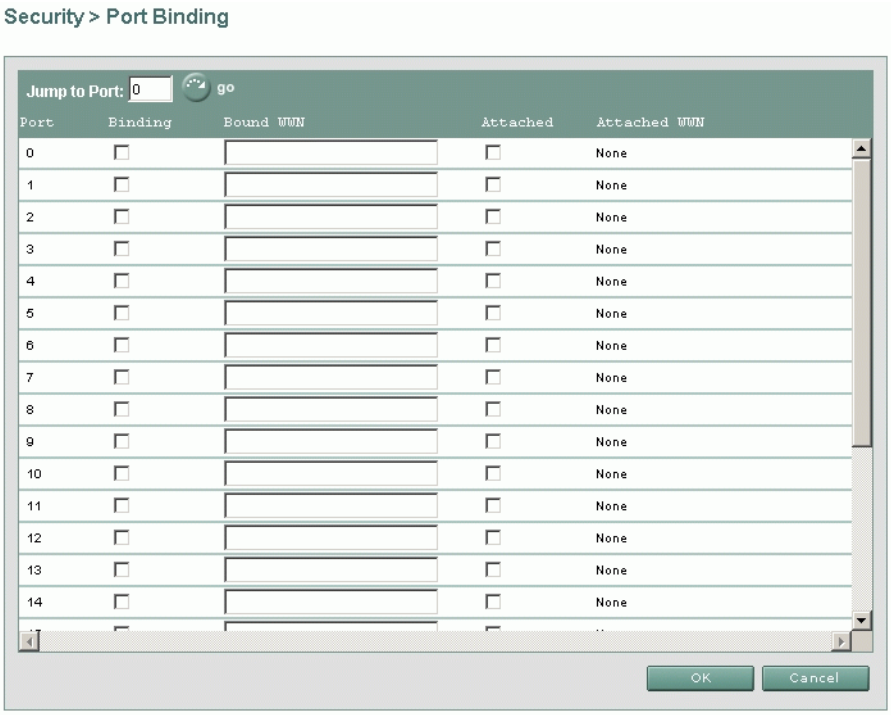


Figure 5-10 Port Binding Page

Use the Port Binding page to configure binding for ports as follows:

1. Click the check box in the *Binding* column next to the port number to enable port binding for the port.
2. Identify the WWN to which the port is bound using one of the following methods:

- Enter the WWN to which the port is to bind in the *Bound WWN* column. The WWN must be entered as hex digits, all uppercase, and you must use a colon to separate digits.
- Click the check box in the *Attached* column. This option is valid only if a WWN is present in the Attached WWN column for the port. (The Attached WWN column indicates the WWN that is currently attached to the port, but is not bound to it.)

ATTENTION! If the *Port Binding* check box is checked, and a WWN is not specified for binding, no devices can attach to the port.

3. Click the *OK* button at the bottom of the screen to activate the configuration changes.

Enabling and Disabling Safe Zoning Mode

Perform this procedure to enable or disable Safe Zoning Mode for the product. When this option is selected, zone merges are prohibited and default zoning is prohibited, if the zone name and zone members in the zone set are not identical.

To enable the Safe Zoning Mode, select the *Safe Zoning Mode* check box on the *Security* menu (Figure 5-11). To disable the Safe zoning Mode, clear the *Safe Zoning Mode* check box on the *Configure* menu.

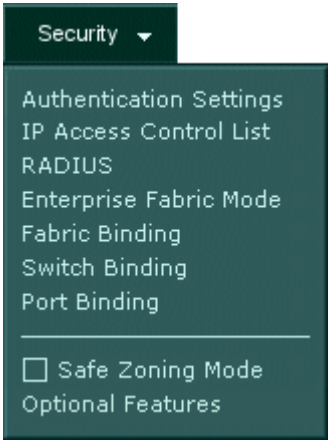


Figure 5-11 Security Menu

Upgrade Options

For information about the *Upgrade Options* command on the *Security* menu, see *Adding Licensed Features* on page 9-2.

6

Viewing System Logs

The commands on the *Logs* menu enable the user to view logs of system and fabric activity.

Each log contains a link that brings the user to a page of ASCII text that reflects the log information present on the machine at that moment. The log displayed is a snapshot of the current log information. Log entries are displayed in the order in which they occurred, with most recent entries listed first. Each log also contains a *Clear Log* button that is used to clear all the entries in the log.

The following logs are available:

- *Viewing the Event Log* 6-2
- *Viewing the Link Incident Log* 6-4
- *Viewing the Audit Log* 6-6
- *Viewing the Security Log* 6-8
- *Viewing the Open Trunking Re-Route Log* 6-10
- *Viewing the Fabric Log* 6-12
- *Viewing the Embedded Port Frame Log* 6-14
- *Viewing All Logs* 6-16
- *Viewing Syslog Configuration* 6-18

Viewing the Event Log

Select *Logs* > *Event* on the navigation panel. The *Event Log* (Figure 6-1) displays. The *Event Log* page provides the following button functions:

- *Clear*—Select this button to clear the contents of the log. The log's contents are deleted from system memory.

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

- *Print*—Select this button to send the contents of the log to a printer.
- *Text File*—Select this button to open the log in a new window as a text file. You can save, edit, or e-mail the file.

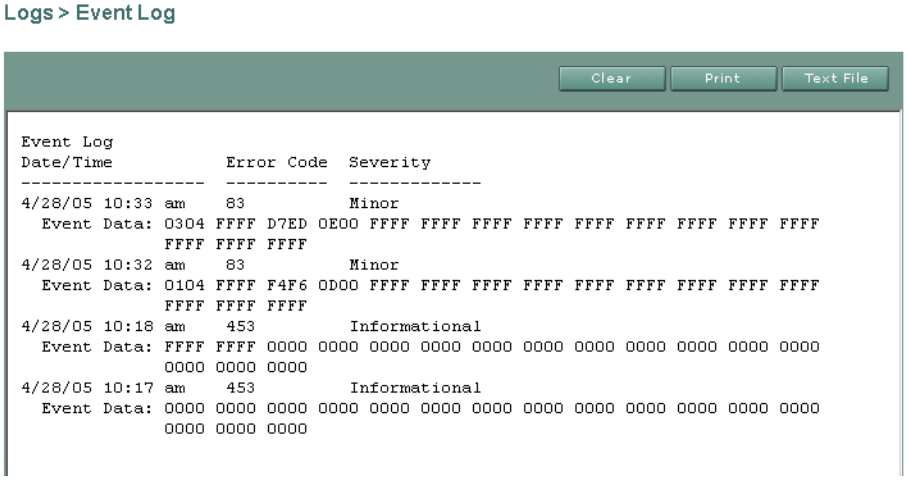

Logs > Event Log
Clear
Print
Text File
Event Log
Date/Time Error Code Severity
4/28/05 10:33 am 83 Minor
Event Data: 0304 FFFF D7ED 0E00 FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
FFFF FFFF FFFF
4/28/05 10:32 am 83 Minor
Event Data: 0104 FFFF F4F6 0D00 FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
FFFF FFFF FFFF
4/28/05 10:18 am 453 Informational
Event Data: FFFF FFFF 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000
4/28/05 10:17 am 453 Informational
Event Data: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000

Figure 6-1 Event Log Page

The Event Log displays a record of significant events that have occurred on the product, such as degraded operation, FRU failures, and port problems. The Event Log is an important tool you can use to monitor and troubleshoot the products in the SAN. Information contained in the event log may also be used by customer support and service personnel to help resolve problems.

The Event Log displays the following information:

- Date/Time: Represents the date and time the event occurred on the switch.
- Error code: Numeric code for the event. For more information, see *Error Event Code Categories* on page 6-3.
- Severity: The severity of the event represented in text. There are four levels, indicating an increasing level of severity: Informational, Minor, Major, and Severe (not operational).
- Event Data: Hexadecimal data provided with the event.

Error Event Code Categories

Error Event Codes define event categories; the categories and events vary by product. Below is a list of event codes:

- 1xx—System events
- 2xx—Power supply events
- 3xx—Fan events
- 4xx—Control processor card events
- 5xx—Port or universal port module card events
- 6xx—Serial crossbar assembly (SBAR) events
- 8xx—Thermal incident events

For detailed information on event codes and isolating problems from event data, refer to the product installation and service manual.

TIP: In addition to the event log, another method to obtain operation information about the status of the product is from the Product Menu. Refer to Chapter 2, *Viewing Product Information*.

Viewing the Link Incident Log

Select *Logs* > *Link Incident* on the navigation panel. The *Link Incident Log* (Figure 6-2) displays. The *Link Incident Log* page provides the following button functions:

- *Clear*—Select this button to clear the contents of the log. The log's contents are deleted from system memory.

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

- *Print*—Select this button to send the contents of the log to a printer.
- *Text File*—Select this button to open the log in a new window as a text file. You can save, edit, or e-mail the file.

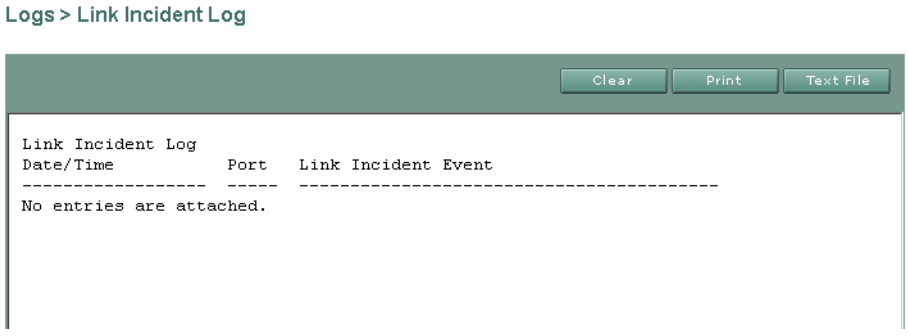


Figure 6-2 Link Incident Log Page

The Link Incident Log provides the following information about link incidents:

- Date/Time: Date and time when the link incident event occurred.
- Port: The port on which the link incident occurred.
- Link Incident Event: An ASCII string describing the link incident event. The following events may cause a link incident to be written to the log:
  - Implicit incident. The attached node detects a condition that may cause problems on the link.

— Bit-error threshold exceeded. The number of code violation errors has exceeded the specified threshold.

— Loss-of-signal or loss-of-synchronization. This occurs if a cable is unplugged from an attached node. Loss-of-signal occurs when a cable is unplugged from an attached node. Loss-of-synchronization is reported if the condition has persisted for longer than the resource allocation time out value (R_A_TOV).

— Not-operational (NOS) primitive sequence received.

— Primitive sequence time out:

- Link reset protocol time out occurred.
- Time out occurred for an appropriate response while in NOS receive state and after NOS is no longer recognized.

— Invalid primitive sequence received for the current link state. Either a link reset or a link reset response primitive sequence was recognized while waiting for the offline sequence.

Viewing the Audit Log

Select *Logs* > *Audit* on the navigation panel. The *Audit Log* (Figure 6-3) displays. The *Audit Log* page provides the following button functions:

- *Clear*—Select this button to clear the contents of the log. The log's contents are deleted from system memory.

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

- *Print*—Select this button to send the contents of the log to a printer.
- *Text File*—Select this button to open the log in a new window as a text file. You can save, edit, or e-mail the file.

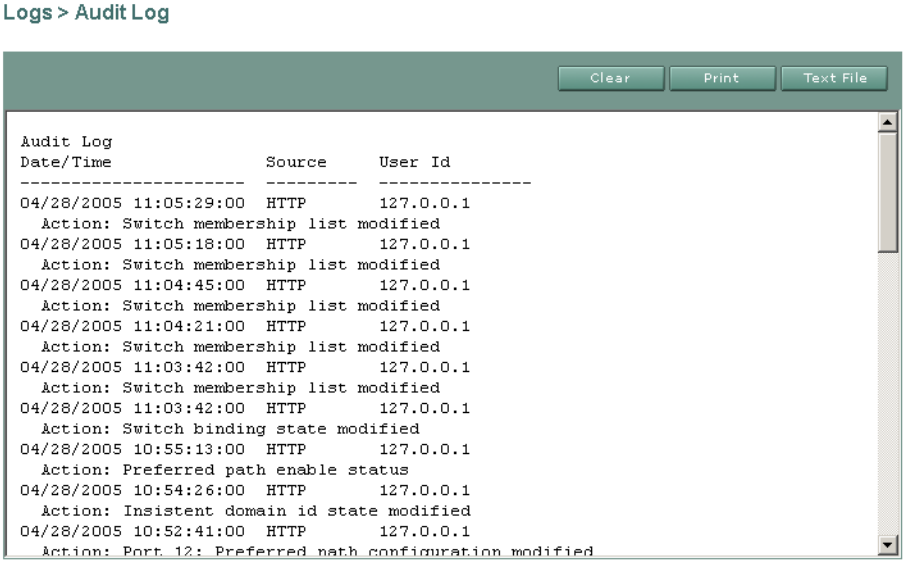

Logs > Audit Log
Clear
Print
Text File
Audit Log
Date/Time Source User Id
04/28/2005 11:05:29:00 HTTP 127.0.0.1
Action: Switch membership list modified
04/28/2005 11:05:18:00 HTTP 127.0.0.1
Action: Switch membership list modified
04/28/2005 11:04:45:00 HTTP 127.0.0.1
Action: Switch membership list modified
04/28/2005 11:04:21:00 HTTP 127.0.0.1
Action: Switch membership list modified
04/28/2005 11:03:42:00 HTTP 127.0.0.1
Action: Switch membership list modified
04/28/2005 11:03:42:00 HTTP 127.0.0.1
Action: Switch binding state modified
04/28/2005 10:55:13:00 HTTP 127.0.0.1
Action: Preferred path enable status
04/28/2005 10:54:26:00 HTTP 127.0.0.1
Action: Insistent domain id state modified
04/28/2005 10:52:41:00 HTTP 127.0.0.1

Figure 6-3 Audit Log Page

The audit log provides:

- Date/Time: The date and time of the log entry.
- Source: The source of Audit Log event.

- User ID: Identifier of the user that issued the command. The identifier is usually an IP address.
- Action: The type of Audit Log event.

Viewing the Security Log

Select *Logs* > *Security* on the navigation panel. The *Security Log* (Figure 6-4) displays. The *Security Log* page provides the following button functions:

- *Clear*—Select this button to clear the contents of the log. The log's contents are deleted from system memory.

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

- *Print*—Select this button to send the contents of the log to a printer.
- *Text File*—Select this button to open the log in a new window as a text file. You can save, edit, or e-mail the file.

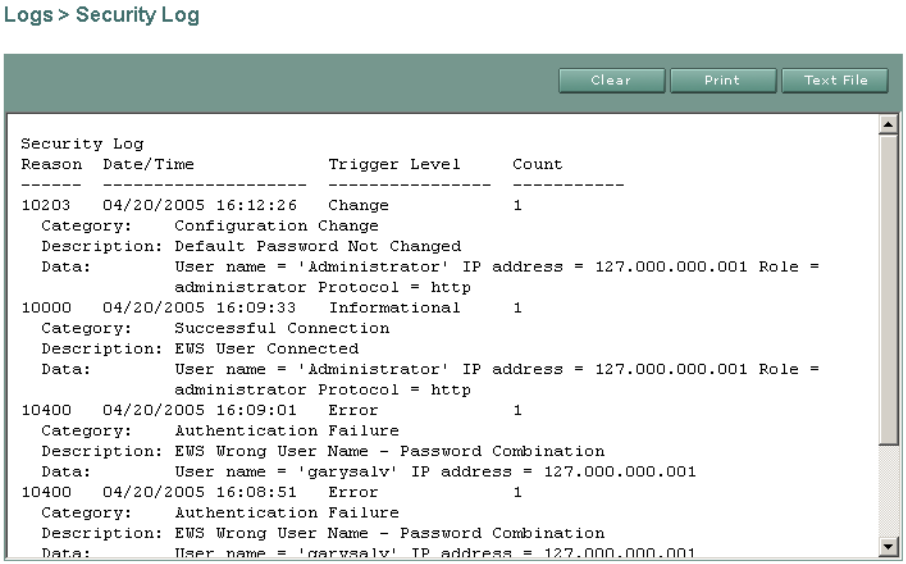

Logs > Security Log
Clear
Print
Text File
Security Log
Reason Date/Time Trigger Level Count
10203 04/20/2005 16:12:26 Change 1
Category: Configuration Change
Description: Default Password Not Changed
Data: User name = 'Administrator' IP address = 127.000.000.001 Role = administrator Protocol = http
10000 04/20/2005 16:09:33 Informational 1
Category: Successful Connection
Description: EWS User Connected
Data: User name = 'Administrator' IP address = 127.000.000.001 Role = administrator Protocol = http
10400 04/20/2005 16:09:01 Error 1
Category: Authentication Failure
Description: EWS Wrong User Name - Password Combination
Data: User name = 'garysalv' IP address = 127.000.000.001
10400 04/20/2005 16:08:51 Error 1
Category: Authentication Failure
Description: EWS Wrong User Name - Password Combination

Figure 6-4 Security Log Page

The security log provides:

- Reason: The reason code for the security event
- Date/Time: The date/time when the event occurred.

- Trigger Level: The trigger level of the event. Possible values include: Informational, Security Change, or Error
- Count: A cumulative count of events within a known period.
- Category: The event category message with possible values may be: Successful Connection, Disconnection, Configuration Change, Authorization Failure, Authentication Failure, or Reserved
- Description: Description of the event.
- Data: Any extra or event specific data.

Viewing the Open Trunking Re-Route Log

Select *Logs* > *Open Trunking Re-Route* on the navigation panel. The *Open Trunking Re-Route Log* (Figure 6-5) displays. The *Open Trunking Re-Route Log* page provides the following button functions:

- *Clear*—Select this button to clear the contents of the log. The log's contents are deleted from system memory.

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

- *Print*—Select this button to send the contents of the log to a printer.
- *Text File*—Select this button to open the log in a new window as a text file. You can save, edit, or e-mail the file.

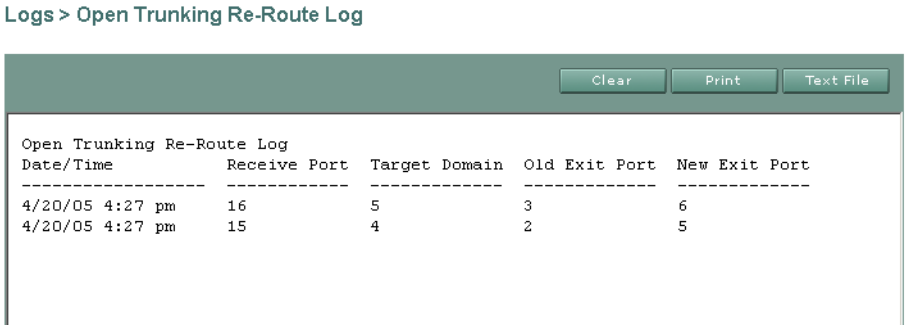

Logs > Open Trunking Re-Route Log
Clear
Print
Text File
Open Trunking Re-Route Log
Date/Time Receive Port Target Domain Old Exit Port New Exit Port
4/20/05 4:27 pm 16 5 3 6
4/20/05 4:27 pm 15 4 2 5

Figure 6-5 Open Trunking Re-Route Log Page

The Open Trunking feature monitors the average data rates of all traffic flows on InterSwitch Links (ISLs) and periodically reroutes data flows from congested links to lightly loaded links. These rerouting activities are recorded in the Open Trunking Re-Route Log.

The Open Trunking Re-Route Log provides the following:

- Date/Time: Date and time when rerouting occurred.
- Receive Port: The decimal receive-port number on the local switch associated with the flow that was rerouted.
- Target Domain: The decimal domain ID associated with the flow that was rerouted.

- Old Exit Port: The decimal exit-port number on this switch that the flow used to get to the target domain.
- New Exit Port: The decimal exit-port number on this switch that the flow now uses to get to the target domain.

Viewing the Fabric Log

Select *Logs* > *Fabric* on the navigation panel. The *Fabric Log* (Figure 6-6) wrapping page displays. The *Fabric Log* page provides the following button functions:

- *Wrapping*—Select this button to display the wrapping page of the log. This page shows the last entries written in the log, because once the log is full, the oldest entries are overwritten with new entries.
- *Non Wrapping*—Select this button to display the non-wrapping page of the log. This page shows the first entries written to the log.

TIP: The same entries will go into both wrapped and non-wrapped logs until the non-wrap log gets full. Once the non-wrap log gets full, the entries go into the wrap log. Once the wrap log is full, it will start to overwrite entries. If you need to look at a history of log entries, you should review both logs.

- *Clear*—Select this button to clear the contents of the log. The log's contents are deleted from system memory.

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

- *Print*—Select this button to send the contents of the log to a printer.
- *Text File*—Select this button to open the log in a new window as a text file. You can save, edit, or e-mail the file.

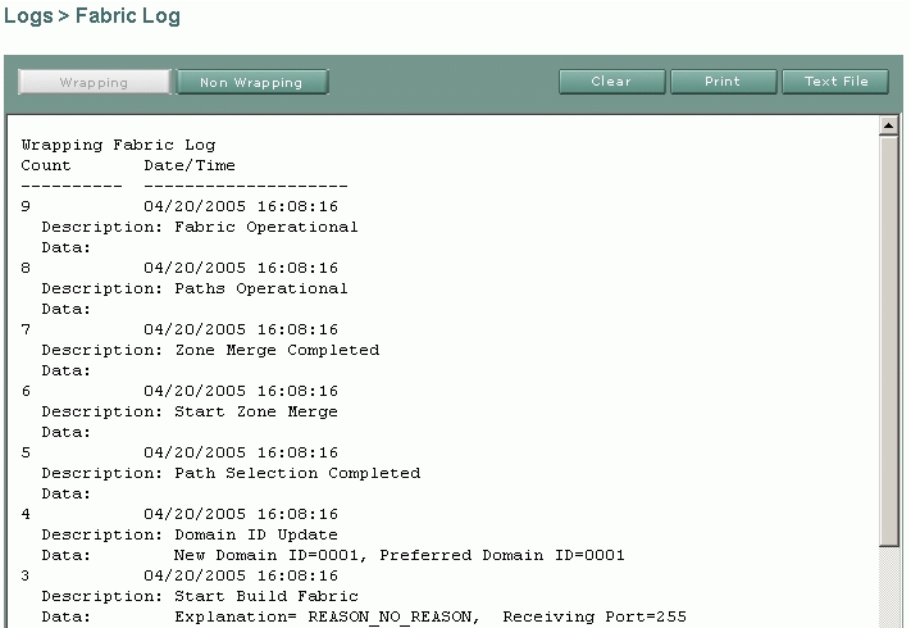


Figure 6-6 Fabric Log Page

The Fabric Log provides:

- Count: A cumulative count of entries within a known period.
- Date/Time: The date and time of the log entry.
- Description: A description of the log entry.
- Data: Extended data that is associated with the log entry.

Viewing the Embedded Port Frame Log

Select *Logs* > *Embedded Port Frame* on the navigation panel. The *Embedded Port Frame Log* (Figure 6-7) page displays. The *Fabric Log* page provides the following button functions:

- *Wrapping*—Select this button to display the wrapping page of the log. This page shows the last entries written in the log, because once the log is full, the oldest entries are overwritten with new entries.
- *Non Wrapping*—Select this button to display the non-wrapping page of the log. This page shows the first entries written to the log.

TIP: The same entries will go into both wrapped and non-wrapped logs until the non-wrap log gets full. Once the non-wrap log gets full, the entries go into the wrap log. Once the wrap log is full, it will start to overwrite entries. If you need to look at a history of log entries, you should review both logs.

- *Clear*—Select this button to clear the contents of the log. The log's contents are deleted from system memory.

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

- *Print*—Select this button to send the contents of the log to a printer.
- *Text File*—Select this button to open the log in a new window as a text file. You can save, edit, or e-mail the file.

You can also define attributes for filtering Class F frames, as described in *Defining Filtering Settings* on page 6-15.

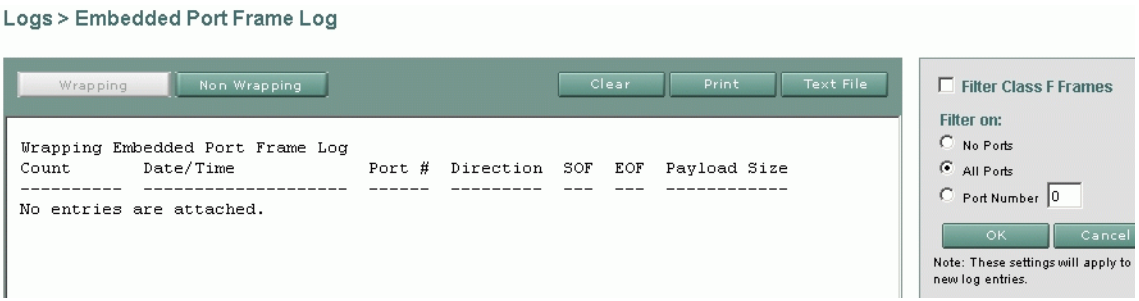


Figure 6-7 Embedded Port Frame Log Page

The Embedded Port Frame Log provides:

- Count: A cumulative count of entries within a known period.
- Date/Time: Date and time of the frame.
- Port #: The port number.
- Direction: Direction of the frame through the port (I = In, O = Out).
- SOF: Start of frame.
- EOF: End of frame.
- Payload Size: Size of the payload.
- Header: The 24-byte FC frame header.
- Payload: The first 32 bytes of the FC frame payload, if applicable.

Defining Filtering Settings

The dialog box on the right side of the page enables you to turn on filtering of Class F Frames and to choose which port to filter on. Changes to these settings take effect immediately, but the changes will apply only new entries to the log.

To enable filtering of Class F frames only, select the *Filter Class F Frames* check box. To disable filtering only on these frames, clear the *Filter Class F Frames* check box.

You can define which ports to filter on by selecting one of the radio buttons in the *Filter on* area:

- *No Ports*—Select this radio button to specify that no ports filter for traffic.
- *All Ports*—Select this radio button to specify that all ports filter for traffic.
- *Port Number*—Select this radio button to specify a single port for filtering of traffic. Enter the port number of the port on which to filter in the corresponding field.

Select the *OK* button to activate changes to frame filtering.

Viewing All Logs

Select *Logs* > *All* on the navigation panel. The *All Logs* page (Figure 6-8) displays. The *All Logs* page provides the following button functions:

- *Clear*—Select this button to clear the contents of all logs on the product. The contents of all logs are deleted from system memory.

ATTENTION! Before clearing all logs, make sure the logs are not needed for troubleshooting. Once the logs are cleared, the data cannot be retrieved.

- *Print*—Select this button to send the contents of the log to a printer.
- *Text File*—Select this button to open the log in a new window as a text file. You can save, edit, or e-mail the file.

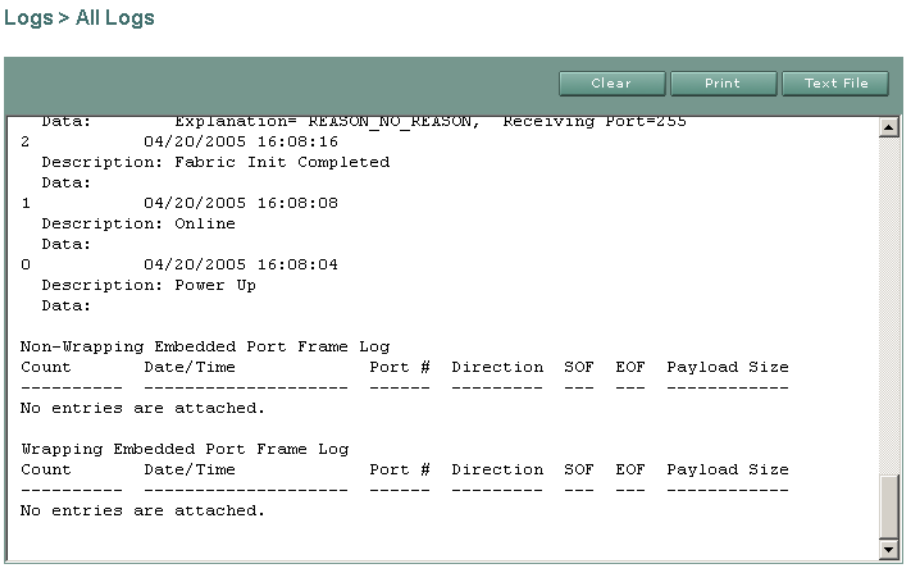


Figure 6-8 All Logs Page

The **All Logs** listing provides the ability to view (display) all of the content of the following logs:

- Event Log—For more information, see *Viewing the Event Log* on page 6-2.
- Open Trunking Re-Route Log—For more information, see *Viewing the Open Trunking Re-Route Log* on page 6-10.
- Link Incident Log—For more information, see *Viewing the Link Incident Log* on page 6-4.
- Security Log—For more information, see *Viewing the Security Log* on page 6-8.
- Audit Log—For more information, see *Viewing the Audit Log* on page 6-6.
- Fabric Log—For more information, see *Viewing the Fabric Log* on page 6-12.
- Embedded Port Frame Log—For more information, see *Viewing the Embedded Port Frame Log* on page 6-14.

Viewing Syslog Configuration

The *Syslog Configuration* page enables you to configure client systems to receive logs from the product. A remote host receives copies of the system logs (syslogs), providing a means to view logs if the product is unavailable.

The recipient clients are identified by IP address. You can specify multiple clients for receiving logs. The interface also enables you to choose which logs the product sends to its syslog recipients.

To configure remote logs, select *Logs* > *Syslog Configuration* on the navigation panel. The *Syslog Configuration* page (Figure 6-9) displays.

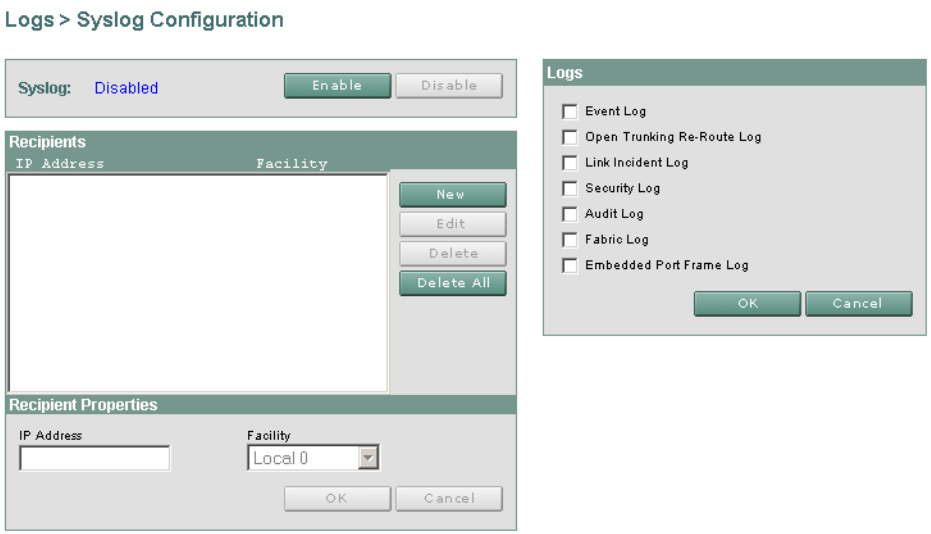


Figure 6-9 Syslog Configuration Page

Use this page to perform the following tasks:

- Enable and disable syslogs, which is described in *Enable and Disable Syslogs* on page 6-19.
- Add a syslog recipient to the list, which is described in *Add a Syslog Recipient* on page 6-19.
- Edit information for a syslog recipient, which is described in *Edit a Syslog Recipient* on page 6-20.

- Delete syslog recipients from the list, which is described in *Delete Syslog Recipients* on page 6-20.
- Identify which logs are sent to recipients, which is described in *Specify Which Logs Are Sent to a Recipient* on page 6-20.

Enable and Disable Syslogs

Sending syslogs to recipients is disabled by default. To enable this functionality, select the *Enable* button. To disable sending syslogs, select the *Disable* button.

Add a Syslog Recipient

The *Recipients* part of the page shows the clients that the product is configured to send syslogs to. The interface allows a maximum of three syslog recipients.

To add an entry to the list, select the *New* button. The *Recipient Properties* dialog becomes active.

Specify the IP address of the syslog recipient in the *IP Address* field.

Select a facility for the syslog recipient by choosing a listing from the *Facility* drop-down list. The facility classifies syslog messages by severity and maps to severity level of events on the product. Specifying a level means that messages at that level and all of greater severity are logged. Valid values for *Facility* and their meaning are shown in Table 6-1.

Table 6-1 Facility Code Levels

Syslog Severity Level	Message Facility Code	E/OS Security Log Level
Local 0	Emergency: system is unusable	N/A
Local 1	Alert: action must be taken immediately	N/A
Local 2	Critical: critical conditions	Error
Local 3	Error: error conditions	N/A
Local 4	Warning: warning conditions	N/A
Local 5	Notice: normal but significant condition	Change
Local 6	Informational	Informational
Local 7	Debug: debug-level messages	N/A

Edit a Syslog Recipient

To change the information for a configured syslog recipient, select the recipient on the list in the *Recipients* area. Select the *Edit* button. The information for the entry is populated to the *Recipient Properties* dialog. Configure the entry's properties as described in *Add a Syslog Recipient* on page 6-19.

Delete Syslog Recipients

To delete a syslog recipient from the list, select an entry from the list in the *Recipients* area. Select the *Delete* button.

To delete all of the configured syslog recipients, select the *Delete All* button.

Specify Which Logs Are Sent to a Recipient

You must identify which logs are sent to syslog recipients using the *Logs* dialog on the right side of the page. To indicate that a log is sent to syslog recipients, select the check box next to the log name and select the *OK* button. To prevent a log from being sent to syslog recipients, clear the check box next to the log name and select the *OK* button.

7

Performing Product Maintenance

The *Maintenance* menu provides commands to perform maintenance tasks, such as port diagnostics. You can access information and tools that are useful in troubleshooting from the *Maintenance* menu.

The following tasks are available on the *Maintenance* menu:

- *Switch Maintenance Tasks* *7-2*
- *Setting Individual Port Beaconing* *7-5*
- *Resetting Ports* *7-6*
- *Performing Diagnostics on a Port* *7-7*
- *Accessing System Files* *7-9*
- *Configuration Backup* *7-11*
- *Configuration Restoration* *7-12*
- *Upgrading Firmware* *7-13*
- *Viewing Product Information* *7-15*
- *Enabling and Disabling Unit Beaconing* *7-17*
- *Clearing the System Error Light* *7-18*
- *HA Power Supplies* *7-18*
- *Upgrade Options* *7-18*

Switch Maintenance Tasks

The *Switch* maintenance page enables you to configure a number of settings for the product on one page.

Select *Maintenance* > *Switch* on the navigation panel. The *Switch* maintenance page (Figure 7-1) displays.

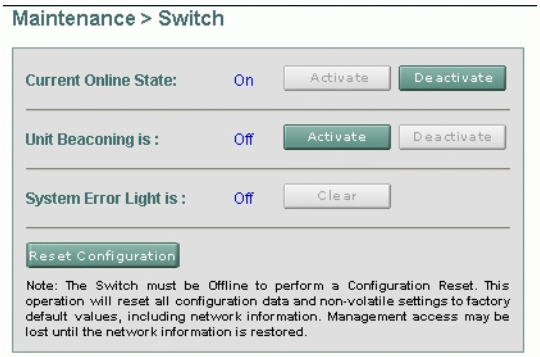

Maintenance > Switch
Current Online State:
On
Activate
Deactivate
Unit Beaconing is :
Off
Activate
Deactivate
System Error Light is :
Off
Clear
Reset Configuration
Note: The Switch must be Offline to perform a Configuration Reset. This operation will reset all configuration data and non-volatile settings to factory default values, including network information. Management access may be lost until the network information is restored.

Figure 7-1 Switch Maintenance Page

The *Switch* maintenance page enables you to perform the following tasks:

- Set the online state of the product, which is described in *Set the Product Online State* on page 7-2.
- Set the unit beaconing state of the product, which is described in *Set the Unit Beaconing State* on page 7-3.
- Clear system error lights for the product, which is described in *Clear System Error Lights* on page 7-3.
- Perform a system configuration reset for the product, which is described in *Perform a System Configuration Reset* on page 7-3.

Set the Product Online State

Using the *Switch* maintenance page, you can set the product online, which means it can communicate with the fabric; or set it offline, which means that it cannot communicate with other devices.

The product's online status is shown in the *Current Online State* field. If the value shown is *On*, you can set the product offline by selecting the *Deactivate* button.

If the value in the *Current Online State* field is Off, you can set the product online by selecting the *Activate* button.

Set the Unit Beaconing State

Using the *Switch* maintenance page, you can enable or disable beaconing on the product. The current state of beaconing for the unit, which is either on or off, is displayed by a flashing LED. Beaconing is useful in helping to isolate problems and locate the product, especially when there are multiple products stacked together, such as in a rack-mount cabinet.

The status of beaconing is shown in the *Unit Beaconing is* field. If the value shown is *On*, the product's beacon LED is flashing. To disable beaconing, select the *Deactivate* button.

If the *Unit Beaconing is* field value is *Off*, the LED is not flashing. To enable beaconing, select the *Activate* button.

Clear System Error Lights

The amber system error light indicator, shown on the *Product Hardware* page, simulates the system error light on the actual switch. When this indicator illuminates, an event has occurred requiring immediate attention, such as the failure of the system, power supply/fan, or port. For more information, see Table 2-1, *Status Indicators*, page 2-3.

The status of the system error light is shown by the *System Error Light is* field. If the status is On, you can clear the system error light by selecting the *Clear* button.

Perform a System Configuration Reset

ATTENTION! Service personnel may ask you to perform this operation to resolve system problems. Review this section completely before performing this operation.

The Reset Configuration button of the Switch Maintenance page enables you to reset product configuration values. This enables you to reset all configuration data and nonvolatile settings to the factory default values including any data that was created from the *Configure* menu and associated pages.

For a list of factory default values, refer to the product's installation and service manual.

ATTENTION! This operation will reset all configuration data and non-volatile settings to the factory default values. All optional features will also be disabled. You will need to activate optional features after completing the product reset.

Before resetting the product, review the kinds of data that will be reset by browsing the *Configure* menu and associated options.

If the product configuration is reset, management access of the product may be lost until the network information is restored. The product must be offline before the configuration can be reset. Refer to *Set the Product Online State* on page 7-2 for instructions for setting the product offline.

ATTENTION! Since the current IP address for the product may not match the factory default values, the Ethernet link between the product and the service processor may drop and not reset. Make sure you record the product's current IP address as you will want to enter that value in the IP Address, under the *Switch Network* configuration page. Refer to *Configuring Network Parameters for the Switch* on page 3-16 for instructions.

After you reset the product configuration, view the product information page as described in *Viewing Product Information* on page 7-15. Save the product information page to a file or print the page to verify the changes you made and to identify the default values.

Setting Individual Port Beaconing

Select *Maintenance* > *Ports* > *Beacon* from the navigation panel. The *Ports Beacon* page displays (Figure 7-2). Use this page to enable or disable beaconing for individual ports. Enabling beaconing helps you to locate a specific port for troubleshooting purposes using the flashing port LED. When there are multiple products stacked together, such as in a rack-mount cabinet, beaconing is useful to help locate a specific port.

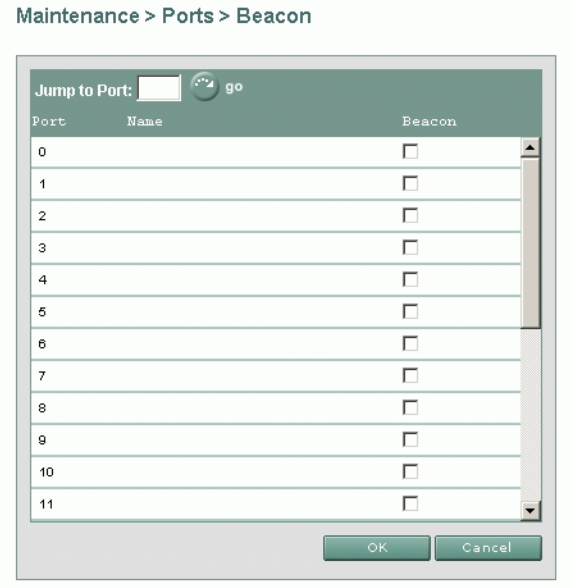


Figure 7-2 Ports Beacon Page

The first column shows the port number, the second column contains the port name, configured as described in *Configuring Basic Port Information* on page 3-2, and the third column contains check boxes to enable/disable beaconing.

A checked box indicates beaconing is active, an empty box indicates beaconing is not active for the port. To set a port to beacon, select the the corresponding check box. (A failed port cannot be set to beacon.) To disable beaconing on a port, clear the corresponding check box. When finished, select the *OK* button to enable the new configuration, or select the *Cancel* button to return to previous configuration.

Resetting Ports

Select *Maintenance* > *Ports* > *Reset* from the navigation panel. The *Ports Reset* page displays (Figure 7-3). Use this page to reset ports. This action clears all statistics counters and disables port beaconing for the port. If a product is attached to the port and is online, this operation sends a link reset to the attached product; otherwise, this action disables port beaconing on the port. If the port is in a failed state, such as after failing a loopback test, the reset restores the port to an operational state and clears the service required (amber) LED. The reset does not affect other ports in the product.

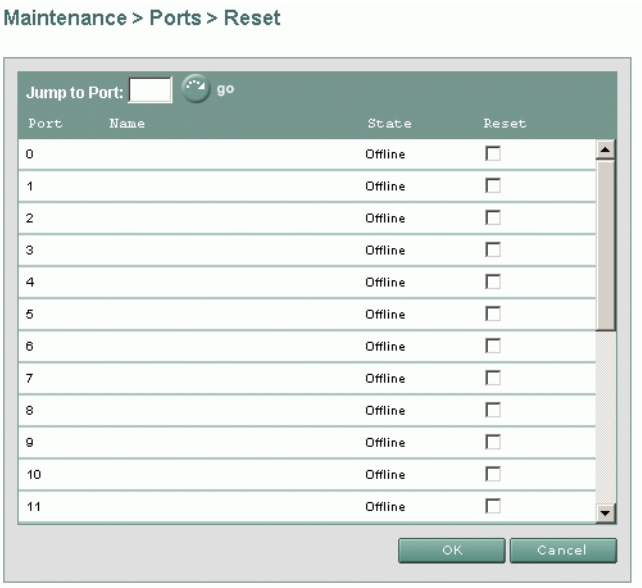


Figure 7-3 Port Reset Page

To reset a port, select the corresponding check box in the *Reset* column. To activate your changes on the product, select the *OK* button.

Performing Diagnostics on a Port

Select *Maintenance* > *Ports* > *Diagnostics* from the navigation panel. The *Ports Diagnostics* page displays (Figure 7-4). Use this page to run either internal or external loopback diagnostic tests for any port. (Service personnel may request these tests to be conducted to aid in troubleshooting problems.) When running port diagnostics, the product may be online or offline and the port can be either blocked or unblocked.

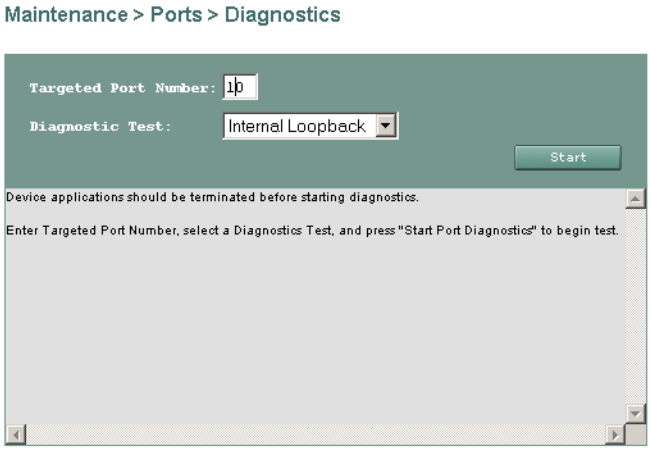

Maintenance > Ports > Diagnostics
Targeted Port Number:
10
Diagnostic Test:
Internal Loopback
Start
Device applications should be terminated before starting diagnostics.
Enter Targeted Port Number, select a Diagnostics Test, and press "Start Port Diagnostics" to begin test.

Figure 7-4 Port Diagnostics Page

Use the following procedure to run a diagnostics test on a port:

1. Select *Maintenance* > *Ports* > *Diagnostics* from the navigation panel. The *Ports Diagnostics* page displays (Figure 7-4).
2. Specify the port on which to run the diagnostic in the *Targeted Port Number* field.
3. Select an option on the Diagnostic Test drop-down menu. Valid options are:
   - **Internal loopback test**—An internal loopback test checks internal port, serializer, and deserializer circuitry.
   - **External loopback test**—An external loopback test checks all port circuitry, including fiber-optic or copper components.
4. Select the *Start* button to initiate the diagnostic test.

5. The *Ports Diagnostics Executing* page (Figure 7-5) displays. This page displays the type of test being run, the port number selected, and a text box that counts down the seconds until the diagnostics are completed. (The test typically lasts 30 seconds.) To discontinue the test, select the *Stop* button.

NOTE: When disconnecting a fiber-optic cable to install an external loopback plug, make sure that you reconnect the cable to the same port after running the external loopback test.

The port's amber LED continues to beacon during the test. If running an internal loopback test, the green LED is off. If running an external loopback test, the green LED is on. Test status displays in the message window and the results display in the status area bar.

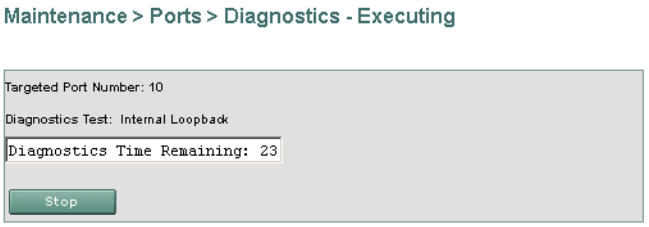

Maintenance > Ports > Diagnostics - Executing
Targeted Port Number: 10
Diagnostics Test: Internal Loopback
Diagnostics Time Remaining: 23
Stop

Figure 7-5 Port Diagnostics - Executing Page

6. When the test completes, the *Ports Diagnostics* page redisplays, showing the results of the test in the *Results* field. Beaconing automatically stops when the test completes or is canceled. If the port fails the test, the port's amber LED remains on.

   If errors occur, record all error information and refer to the product service documentation for problem isolation.

Accessing System Files

The System Files page enables you to access the dump file and the data collection file.

If the operational firmware detects a critical error, the product automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the Control Processor (CTP) card. The CTP dump file contains this maintenance information. The CTP dump file will usually be requested by service personnel to aid in troubleshooting. The process for retrieving the file is documented under *Retrieve the Dump File* on page 7-9.

The data collection file contains information about the current state of the product. This information is collected when you perform the procedure described under *Create the Data Collection File* on page 7-10.

Retrieve the Dump File

Use the following procedure to retrieve the dump file:

1. Select *Maintenance* > *System Files* from the navigation panel. The *System Files* page displays (Figure 7-6).

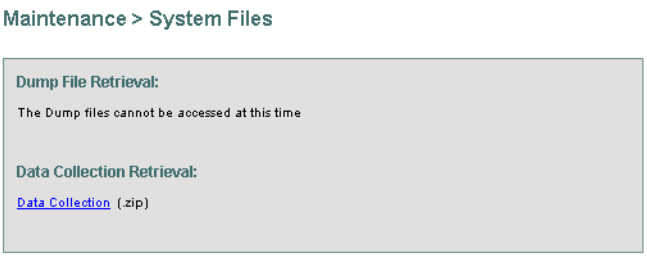

Maintenance > System Files
Dump File Retrieval:
The Dump files cannot be accessed at this time
Data Collection Retrieval:
Data Collection (.zip)

Figure 7-6 System Files Page

2. If no dump file is available, the message **The dump files cannot be accessed at this time** displays. If a dump file is available, right-click the link and select the *Save As* option.
3. When you have accessed the *Save As* dialog box (Figure 7-7 on page 7-10), select *All Files* from the *Save as type:* field. When naming the file, add a **.dmp** extension to the filename.

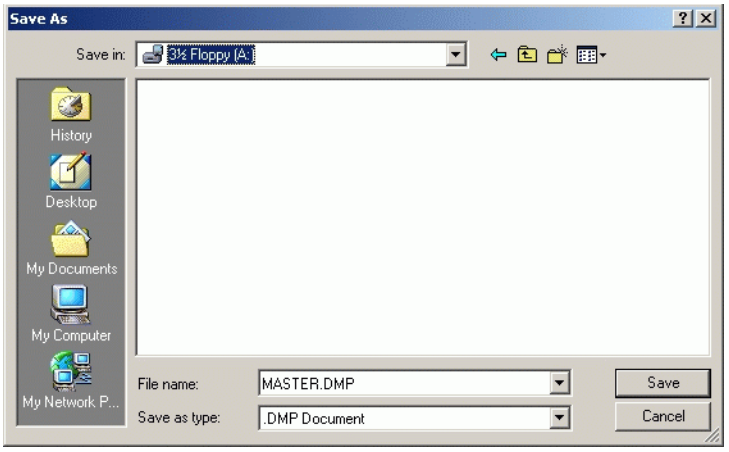


Figure 7-7 Selecting the Location to Save the CTP Maintenance Information

4. When the file is completely downloaded, the Download Complete screen displays. If you encounter any problems during this procedure, contact your service representative.

Create the Data Collection File

Use the following procedure to create the data collection file:

1. Select *Maintenance* > *System Files* from the navigation panel. The *System Files* page displays (Figure 7-6).
2. Right-click on the *Data Collection* link. Select the *Save As* option. Note that the file is a zip file and it will be different sizes between different products.
3. Use the *Save As* dialog box (Figure 7-7 on page 7-10) to select the location for the file. Select the *Save* button.
4. When the file is completely downloaded, the *Download Complete* screen displays. If you encounter any problems during this procedure, contact your service representative.

Configuration Backup

The *Backup Configuration* page enables you to save the current persistent state of the product (the NVRAM contents) to a file in XML format. To perform the backup, you must stop any other management operations; in particular you should not edit a zone set using either the EFCM Basic interface or the CLI.

Follow these steps to back up configuration information:

1. Select *Maintenance* > *Backup Configuration* from the navigation panel. The *Backup Configuration* page displays (Figure 7-8).

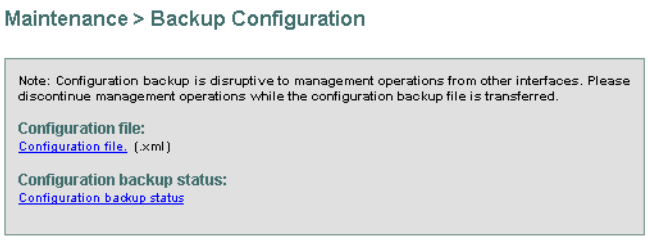

Maintenance > Backup Configuration
Note: Configuration backup is disruptive to management operations from other interfaces. Please discontinue management operations while the configuration backup file is transferred.
Configuration file:
Configuration file. (.xml)
Configuration backup status:
Configuration backup status

Figure 7-8 Backup Configuration Page

2. To begin the file download, right-click on the *Configuration file* link and select the *Save As* option.
3. Use the *Save As* dialog box select a location to save the file. The default file name is `swconfig.xml`.
4. When the file download has completed, you can select the *Configuration backup status* link to determine if any errors occurred during the backup. Typically, the only error possible is a warning that the zone set was modified during backup, possibly leading to a corrupted copy of the zone set in the backup file.

Configuration Restoration

The *Restore Configuration* page enables you to download a configuration file from a location that you specify. (The configuration file is created using the procedure described in *Configuration Backup* on page 7-11.)

Follow these steps to download the configuration file:

1. Set the product offline as described in *Switch Maintenance Tasks* on page 7-2.
2. Select *Maintenance* > *Restore Configuration* from the navigation panel. The *Restore Configuration* page displays (Figure 7-9).

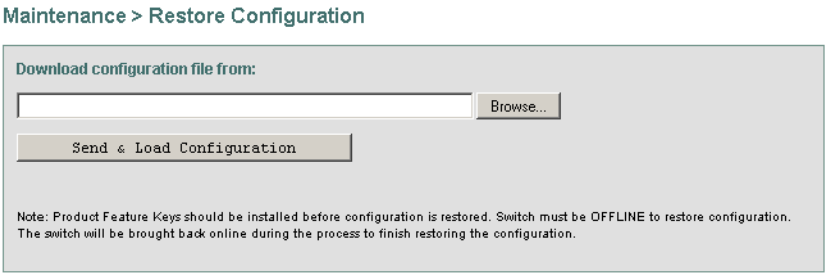

Maintenance > Restore Configuration
Download configuration file from:
Browse...
Send & Load Configuration
Note: Product Feature Keys should be installed before configuration is restored. Switch must be OFFLINE to restore configuration.
The switch will be brought back online during the process to finish restoring the configuration.

Figure 7-9 Restore Configuration Page

3. Select the *Browse* button to open a dialog to select the configuration file.
4. Select the *Send & Load Configuration* button to load the configuration settings in the selected file to the product.

Upgrading Firmware

The *Firmware Upgrade* page enables you to upload and upgrade firmware.

The firmware version shipped with the product is provided on the *System Version XX.YY.ZZ* diskette. McDATA's web site, under *Services*, *Support Login*. (You will need a member name and password to log in.)

Detailed instructions on how to locate and download firmware are provided in the product's installation and service manual.

ATTENTION! When adding a firmware version, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the firmware version. That information supplements and supersedes information provided in this manual.

ATTENTION! Refer to the software release notes on whether the firmware upgrade can be done without causing a disruption as some upgrades may cause a temporary disruption to product function.

Follow these steps to download the configuration file:

1. Select *Maintenance* > *Firmware Upgrade* from the navigation panel. The *Firmware Upgrade* page displays (Figure 7-10 on page 7-13).

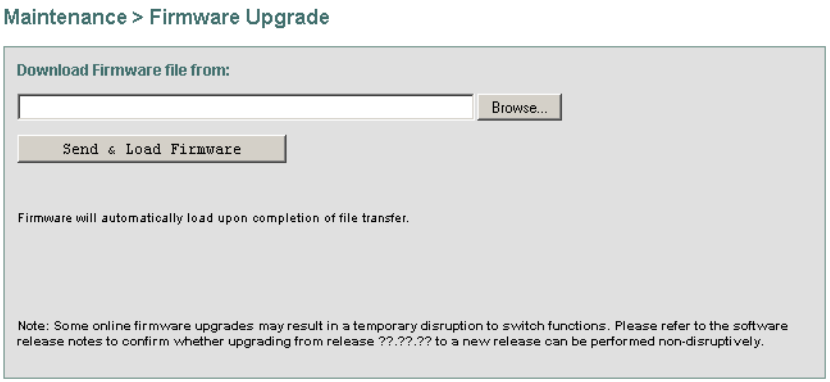

Maintenance > Firmware Upgrade
Download Firmware file from:
Browse...
Send & Load Firmware
Firmware will automatically load upon completion of file transfer.
Note: Some online firmware upgrades may result in a temporary disruption to switch functions. Please refer to the software release notes to confirm whether upgrading from release ??.??.?? to a new release can be performed non-disruptively.

Figure 7-10 Firmware Upgrade Page

2. Type the drive and pathname of the firmware file in the *Download configuration file from* field, or click *Browse* to locate the file.
3. When the correct filename is in the box, click *Send & Load Firmware*. When the firmware has finished transferring, a message displays stating that the new firmware is being activated on the product and the product will be unavailable temporarily. You must reconnect to the EFCM Basic interface after this period by logging back into EFCM Basic.

TIP: You can verify the firmware was upgraded by viewing firmware level shown on the *Fabric View.* Refer to Chapter 8, *Using the Fabric View*.

Activating Optional Features

Activating licensed features is a separate procedure from upgrading firmware. This procedure is described in *Adding Licensed Features* on page 9-2.

Viewing Product Information

The *Product Info* page displays information about the product. To view the product information, select *Maintenance* > *Product Information* from the navigation panel. The *Product Info* page displays (Figure 7-11).

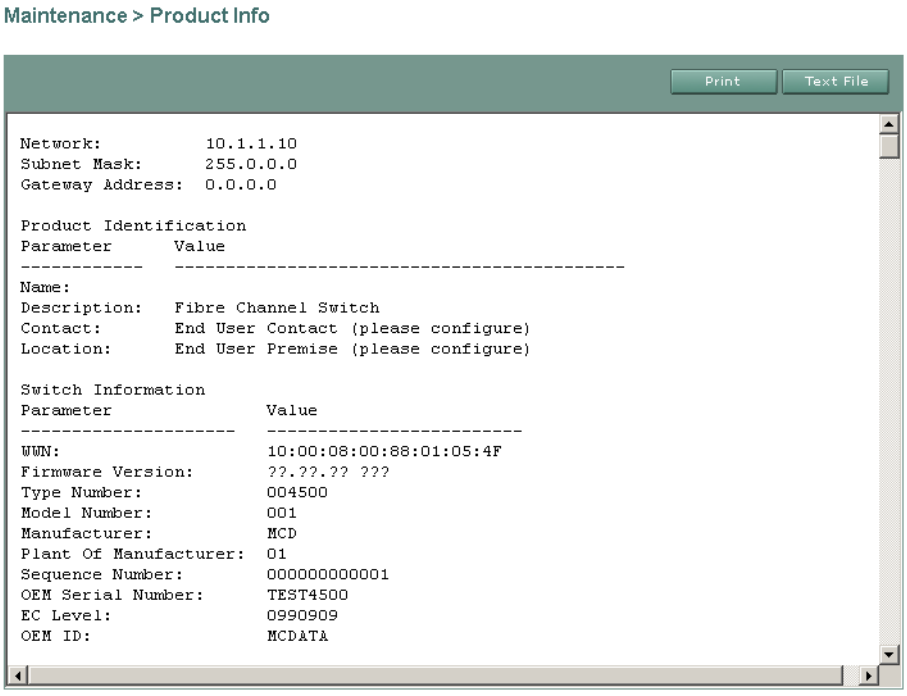


Figure 7-11 Product Information Page

Information shown in this page may be requested by technical support to help resolve technical problems. You can print the file by selecting the *Print* button. You can save this page to a file by selecting the *Text File* button. (You may also want to enter a date in the file or on the printed page to note when the product information file was created.)

The *Print Info* page shows the following information:

- Network Information (IP Address, Subnet Mask, Gateway Address)
- Product Identification Information
- Switch Information
- Switch Parameters
- Fabric Parameters
- Port Configurations
- FRU List and Information
- SNMP Agent State
- Zoning Information
- Port Data
- Port Technology
- Port Login Data
- E_Port State
- BB Credit
- Preferred Path
- Switch Status
- Switch Configuration
- Installed Features
- Port Binding
- Switch Binding
- Fabric Binding
- Authentication Users Database
- Authentication Settings
- Switch IP Access Control List
- Authentication Ports
- RADIUS
- Open Trunking Configuration

- Threshold Alerts
- Fabric Topology
- Fabric Node List
- Port Fencing

Enabling and Disabling Unit Beaconing

Beaconing is useful in helping to isolate problems and locate the product, especially when there are multiple products stacked together, such as in a rack-mount cabinet. When unit beaconing is enabled, the product's beacon LED flashes.

To enable beaconing, select the *Unit Beaconing* check box on the *Maintenance* menu (Figure 7-12). To disable beaconing, clear the *Unit Beaconing* check box on the *Maintenance* menu.

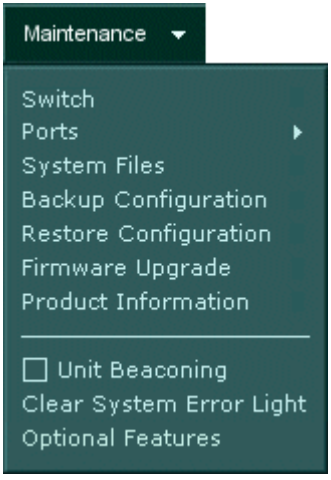


Figure 7-12 Maintenance Menu

Clearing the System Error Light

The amber system error light indicator, shown on the *Product Hardware* page, simulates the system error light on the actual switch. When this indicator illuminates, an event has occurred requiring immediate attention, such as the failure of the system, power supply/fan, or port. For more information, see Table 2-1, *Status Indicators*, page 2-3.

To clear the system error light, select *Clear System Error Light* on the *Maintenance* menu (Figure 7-12).

HA Power Supplies

The 16-Port 4-Gbps Switch can have a High Availability (HA) power supply, but it must be enabled.

To enable the product's HA power supply, you must first verify that both power supplies for the product are plugged in. Then select the *HA Power Supplies* check box on the *Maintenance* menu. (This menu option is available only on the 16-Port 4-Gbps switch.)

To disable HA power for the product, clear the *HA Power Supplies* check box.

Upgrade Options

For information about the *Upgrade Options* command on the Configure menu, see *Adding Licensed Features* on page 9-2.

8

Using the Fabric View

The following information about the *Fabric View* is available:

- *Overview of the Fabric View* *8-1*
- *Fabric View Elements* *8-1*

Overview of the Fabric View

The *Fabric View* is the first screen displayed after logging into the EFCM Basic interface. The *Fabric View* page (Figure 8-1, *Fabric View with 10 Domain IDs*, on page 8-2) is presented from the perspective of the IP Address entered in by the user during system login. This page serves as a view of the current topology of the fabric and as a gateway for accessing switches in the fabric.

Fabric View Elements

The *Fabric View* interacts with products in the fabric (other than the one you are logged into) using a set of in-band requests to the product. The in-band communication originates from the current switch (the product that you logged into). The current switch is identified by the IP address listed in the *Topology from* field. The point-of-view of the information shown in this page is that of the current switch.

The *Fabric View* shows devices in the fabric in two locations, the *Fabric Tree* on the left side of the page and the *Product Boxes* on the right side of the page.

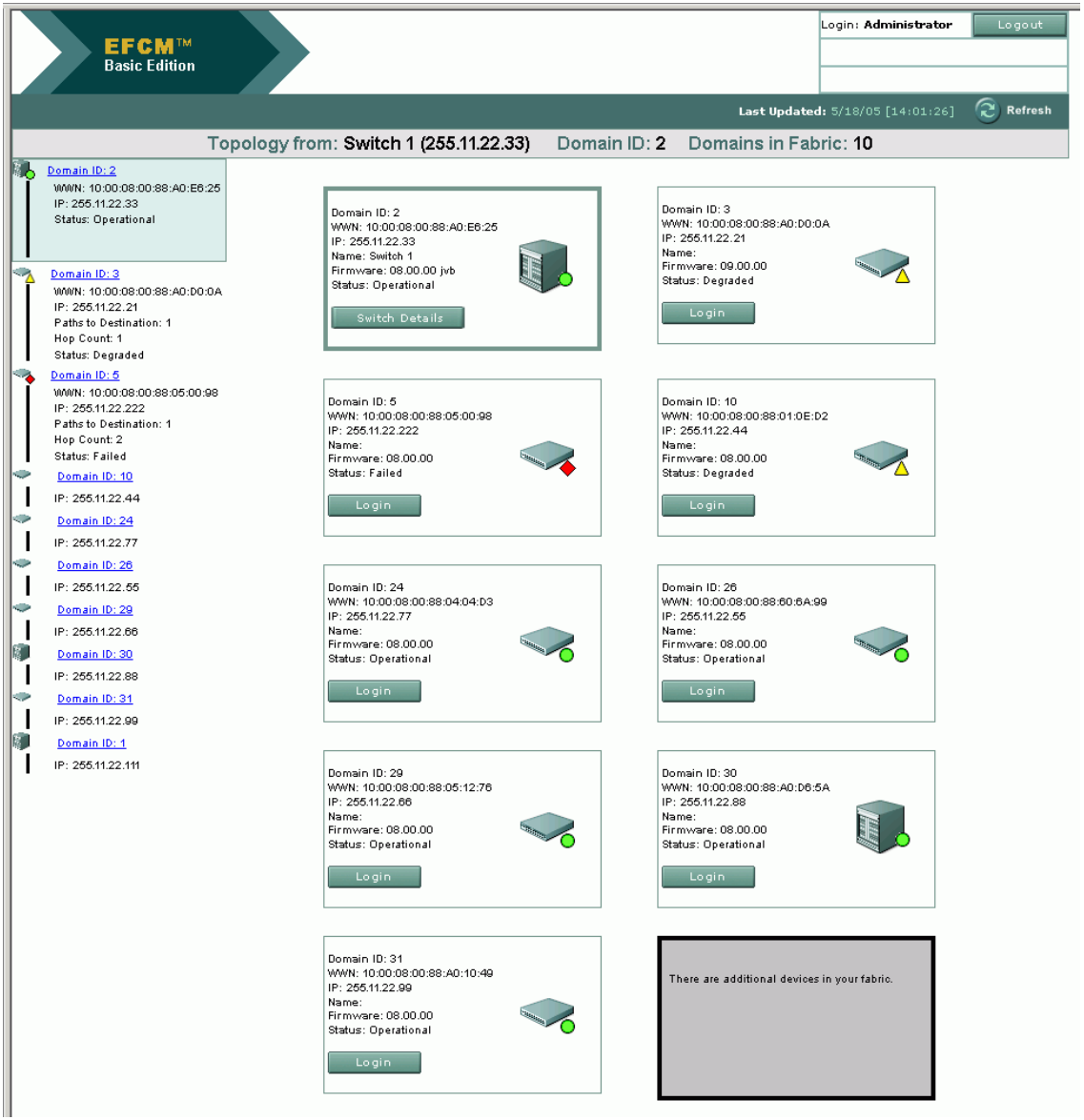


Figure 8-1 Fabric View with 10 Domain IDs

Fabric Tree

The panel on the left of the page is a fabric tree of all the domains in the fabric sorted by domain ID in numerical order. The fabric tree

cannot be expanded or contracted. The listings in the fabric tree provide the following information, for the current product and the next two domain IDs:

- *Domain ID* —This field is a link that opens the *Product Hardware* page for the corresponding device.
- *WWN*—World Wide Number (WWN) of the switch/domain.
- *IP*—IP address of the switch/domain.
- *Paths to Destination*—The number of paths to this product/domain ID from the perspective of the product you are logged into.
- *Hop Count*—Number of network hops to this product/domain ID from the perspective of the product you are logged into.
- *Status*—Operational status of the switch.

Listings for domain IDs other than the three products do not contain the above information.

The links for these domain IDs forward the user to the *Upgrade* page, because, if your SAN contains more than three devices, the EFCM Basic interface may not be appropriate for your SAN management requirements. (For a description of the *Upgrade* page, see *Software Upgrade and Feature Installation* on page 9-1.)

To access devices not shown in the page, you must login using the IP address of a device that has a domain ID that will result in the information you want to view.

Product Boxes

The *Fabric View* page can display a maximum of nine product boxes. The order of devices shown on this page is numeric by domain ID, starting with the domain ID belonging to the IP address that was logged into by the user. All other devices are shown in the Fabric Tree, but are not available as Product Boxes.

To access devices not shown in the page, you must login using the IP address of a device that has a domain ID that will result in the information you want to view.

Up to nine products display in the boxes on the right side of the page. The box of the current switch is shaded green. The following information is displayed for these products:

- *Domain ID*—Domain ID of the corresponding device.

- *WWN*—WWN of the switch/domain.
- *IP*—IP address of the switch/domain.
- *Name*—Name of the switch as configured by the user.
- *Firmware*—Firmware release version.
- *Status*—operational status of the switch (Operational, Degraded, or Failed).
- *Switch Details* button—Available only for the current product, This button opens the *Product Hardware* page for the corresponding device and enables the drop-down menus that are used to configure and monitor the device.
- *Login* button—This button opens a login dialog for the selected product.

If more than nine switches are present in the fabric, a box displays in the right panel stating that additional devices are in the fabric.

9

Software Upgrade and Feature Installation

Because the EFCM Basic interface provides a limited amount of SAN management capacity, and SANs frequently grow, the interface has functionality intended to aid you in upgrading your SAN management capacity. The EFCM Basic interface provides two methods of upgrading your system's SAN Management technology:

- Adding functionality using EFCM Basic licensed features, as described in *Adding Licensed Features* on page 9-2.
- Upgrading to a SAN management system more appropriate to a large-scale SAN, as described in *Upgrading Your SAN Management System* on page 10-1.

Adding Licensed Features

Select *Optional Features* from the *Configure*, *Security*, or *Maintenance* menus. The *Maintenance Feature Installation* page displays (Figure 9-1). This page provides a list of the licensed features that are available on the system.

Select an entry in the Features panel to view information about the feature. In the *Installed* column, a check mark indicates that the feature is currently installed on the product, and an *X* indicates that the feature is not installed. (The number of ports licensed on the product displays for the *Flex Ports* entry.) The licensed features are described in *Licensed Features* on page 9-3.

The page also provides an interface for upgrading your system's functionality, by entering a feature key. This procedure is described in *Entering a Feature Key* on page 9-3.

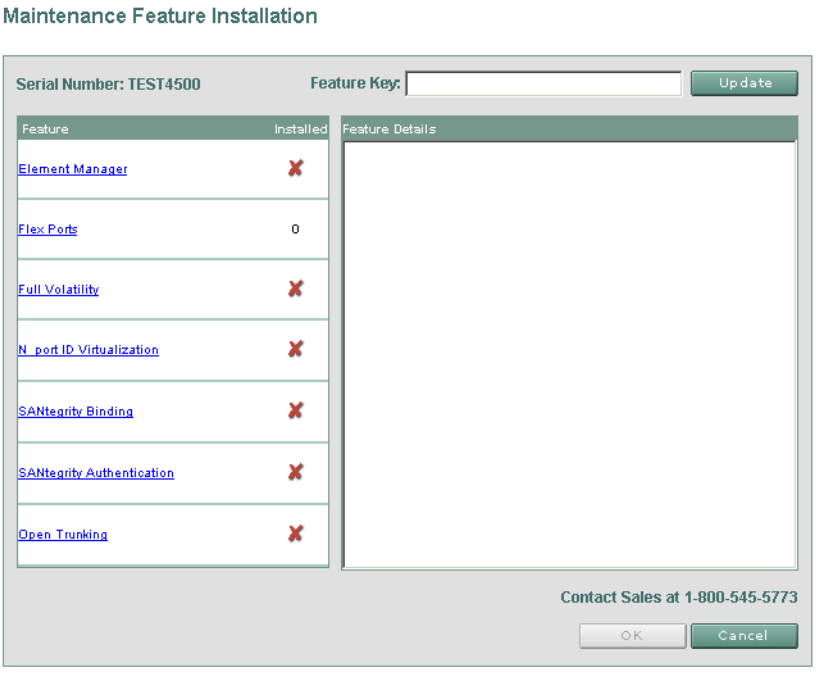


Figure 9-1 Maintenance Feature Installation Page

Licensed Features

The licensed features are:

- **Element Manager**—This feature enables the EFCM Element Manager for the product.
- **Flexport**—A Flexport switch is delivered at a discount with only a portion of the switch's ports enabled. When additional port capacity is required, the remaining ports are enabled through purchase of this feature. Ports are enabled in increments of eight, except for the 12-Port Switch, for which ports are enabled in groups of four.
- **Full Volatility**—This feature is a security feature that supports military, classified, or other high-security environments that require that Fibre Channel data not be retained by the product after power off or failure.
- **N_port ID Virtualization**—This feature allows you to assign multiple Fibre Channel addresses (N_port IDs) to a single physical N_port.
- **SANtegrity™ Binding**—This feature enhances security in SANs, which is valuable in SANs that contain a large or heterogeneous group of fabrics and attached devices. Through these features, you can allow or prohibit switch attachment to fabrics and device attachment to switches and directors. Aspects of SANtegrity Binding include fabric binding, switch binding, and Enterprise Fabric Mode.
- **SANtegrity™ Authentication**—This feature enhances security of the product by controlling the ability of users, devices, and processes to attach to the product.
- **OpenTrunking**—This feature enhances efficiency in the use of redundant ISLs between neighboring switches by means of load balancing. This prevents traffic from becoming congested on an ISL.

Entering a Feature Key

To obtain a feature license key, follow instructions provided with your product's ship kit to log into a customer web site through your internet browser, enter the serial number and transaction code provided with your ship kit, and obtain a license key.

A feature license key is an alphanumeric string consisting of both uppercase and lowercase characters. The total number of characters

may vary depending on keys and serial number. The feature key is case sensitive and must be entered exactly, including dashes.

Feature keys use a format similar to the following:

XxXx-XXxX-xxXX-xX.

TIP: You must be logged in with Administrator-level rights to install feature keys.

The feature key can be installed while the product is online, unless the new feature key removes existing functionality. If functionality is removed by the feature key, the product must be offline.

Use the following procedures to enable the new features:

1. To install a feature, select *Optional Features* from the *Configure*, *Security*, or *Maintenance* menus. The Maintenance Feature Installation page displays (Figure 9-1 on page 9-2).
2. Enter the feature key in the *Feature Key* field and select the *Update* button. The interface displays a confirmation page with a warning, stating this action overrides the current set of product features.

ATTENTION! When *Update* is selected, all current features are removed and replaced with the features specified in the feature key. Features not included in the new feature key are no longer available on the system. Because of this, it is important to verify that the feature key enables all desired features.

---

3. Click *Update* to activate the new feature key. (The system automatically undergoes an IPL.)

ATTENTION! If you receive the error message `Error 238, Invalid Key`, either the feature key was entered incorrectly or the feature key is not valid for that feature. Re-enter the feature key. If you continue to have problems, contact technical support.

10

Upgrading Your SAN Management System

Differences Between EFCM Basic and other McDATA Products

The EFCM Basic interface is designed to manage products in a simple SAN while the Enterprise Fabric Connectivity Manager (EFCM) and SANavigator are designed to manage products in large scale SANs. Therefore, as you add additional products to your SAN, consider migrating from EFCM Basic to other McDATA management products to provide more efficient management of your SAN.

NOTE: For detailed information, contact your sales representative or visit McDATA's web site, www.mcdata.com.

For information about EFCM, see *Enterprise Fabric Connectivity Manager* on page 10-1.

For information about SANavigator, see *SANavigator* on page 10-2.

Enterprise Fabric Connectivity Manager

Enterprise Fabric Connectivity Manager (EFCM) is a comprehensive storage resource management application used to configure SANs. EFCM simplifies SAN management, optimizes storage resources, and minimizes storage networking risks. When comparing EFCM Basic to EFCM, consider the following attributes of EFCM:

- Enables SAN management from a single console. Systems administrators have the ability to view and zone components in the SAN, as well as remotely adding, removing, or modifying McDATA's interconnected directors and switches.
- Integrates with leading multi-vendor applications. EFCM allows easy integration with heterogeneous applications and environments such as SANavigator™, Veritas, and Tivoli, enabling proactive SAN management.
- Delivers enterprise-class scalability without compromising performance. EFCM is designed to scale from department-level SANs to enterprise networks.
- Offers high levels of access and security. EFCM allows multiple levels of access so only authorized users can change and configure zones and zone sets.
- Streamlines troubleshooting processes. EFCM provides proactive alerts with call-home and e-mail notification capabilities. Systems administrators receive detailed, real-time logging, and diagnostic and fault-isolation data, resulting in accelerated troubleshooting efforts and swift problem resolution.

SANavigator

SANavigator is a powerful storage network management platform that addresses the entire lifecycle of a SAN. From fabric planning and device discovery to storage network configuration and monitoring, SANavigator software makes network storage management easy. It can help you plan, discover, configure and monitor the many components and technologies that make up your multi-vendor storage network infrastructure. When comparing EFCM Basic to SANavigator, consider the following attributes of SANavigator:

- Rapidly identifies all SAN devices and their connections, creating an intuitive visual map.
- Monitors and configures all devices regardless of vendor or protocol.
- Simplifies SAN management through advanced planning and automation tools.
- Maximizes SAN return on investment (ROI) by reducing downtime and minimizing time to resolve issues.

- Leverages existing resources to reduce hardware and personnel costs.
- Minimizes risk through centralized planning and management.

Features and Functions

Performance Monitoring

Measure the performance trends of every switch port in the SAN and pinpoint bandwidth bottlenecks with the SANavigator Performance Monitoring module. Real-time link throughput, error rate, and latency monitoring provide instant awareness of any storage network degradation or failure. Maximize the performance of your storage network with the SANavigator Performance Module.

Event Management

In today's business climate of reduced budgets and diminishing headcounts, SANavigator's event manager provides a compelling return on investment. SANavigator's powerful event and schedule-driven event management module reduces manual intervention and help make the most efficient use of your storage network. Once the policies are in place, SANavigator can automate routine tasks such as report generation and device failure response so that you have faster response time and can be freed up to focus on other issues.

Planning

Widely acknowledged as the best planning tool in the industry, the SANavigator Planning module helps you design a scalable, cost-effective storage network that's perfectly suited to your needs. Verify storage network models before you implement them to increase your ROI and save valuable time and money.

Connectors

No single element is as important to business operations as application data exchange. McDATA connectors act as an interface, providing the necessary infrastructure for SANavigator to share its knowledge of the fabric with higher-level network management framework applications. Available modules: HP OpenView NNM, BMC Patrol, CA Unicenter TNG, Tivoli Netview.

LUN Management

The SANavigator LUN Management module gives you the ability to manage the LUNs on storage arrays from EMC, HDS and IBM. With this module, you'll get the increased data security features associated with LUN masking as well as the ability to create new LUNs on supported storage arrays. Simplify your SAN by using a single application for complete end-to-end management.

Management Features Provided by EFCM and/or SANavigator

Key to large-scale product and SAN management are the following additional features and functions that are available in EFCM and/or SANavigator. Review this list to help you determine if you want to migrate to either EFCM and/or SANavigator. Make sure you consider not just your current implementation but also your future implementation to determine the importance of these features and functions to your SAN implementation. Consult with your sales representative for further information about features and functions provided by EFCM and SANavigator.

Configuring the Product

- User rights for maintenance
- User profiles
- Date time synchronization
- Zone set libraries

Maintaining the Product

- Auto backup of product configuration
- Back up and restore of current product configuration
- Validation of firmware upgrade
- Full data collection of product maintenance information
- FRU beaconing
- LIN alerts
- LIN incident status
- Call home functionality
- E-mail notification

- Remote notification test
- Continuous screen alert indicator
- Dial-in support
- Link incident logs
- Product change status log
- User session logs
- Audit log of user actions
- Export log files

Monitoring System Performance

- Switch between fabric views
- Switch between topology views
- Real-time performance graphs

A

Error Messages

This appendix lists and explains error messages for EFCM Basic. Any error numbers that are not listed are reserved for future use.

The message that is returned is a string that includes the error number and the text of the message.

Message **Error 000: Authorized OK**

Description Informational only.

Action Informational only.

Informational only.

Message **Error 001: Validated OK**

Description Informational only.

Action Informational only.

Message **Error 002: Completed OK**

Description Informational only.

Action Informational only.

Message	**Error 003: Initiated OK**
Description	Informational only.
Action	Informational Only

Message	**Error 004 Busy**
Description	The switch cannot process any requests at this time.
Action	Re-submit the request.

Message	**Error 005: Busy**
Description	The switch cannot process any requests at this time.
Action	Re-submit the request.

Message	**Error 007: Not Authorized**
Description	You are unable to get write authorization to save the configuration.
Action	Try again later.

Message	**Error 006: In Allegiance**
Description	Informational Only.
Action	Informational Only

Message	**Error 008: Invalid Switch Name**
Description	The value entered for the switch name is invalid.
Action	The name for the director or switch may contain 0–24 characters. Enter a name with 0–24 characters and re-submit.

Message **Error 009: Invalid Switch Description**

Description The value entered for the switch DESCRIPTION is invalid.

Action The description for the director or switch may contain 0–255 characters. Enter a description with 0–255 characters and re-submit.

Message **Error 010: Invalid Switch Location**

Description The value entered for the switch location is invalid.

Action The location for the director or switch may contain 0–255 characters. Enter a location with 0–255 characters and re-submit.

Message **Error 011: Invalid Switch Contact**

Description The value entered for the switch contact is invalid.

Action The contact for the director or switch may contain 0–255 characters. Enter a contact with 0–255 characters and re-submit.

Message **Error 012: Invalid Port Address**

Description The value entered for the port address is invalid.

Action Enter a port address within the range supported by your director or switch.

Message **Error 013: Invalid Port Number**

Description The value entered for the port number is invalid.

Action Enter a port number within the range supported by your director or switch.

Message **Error 014: Invalid Port Name**

Description The value entered for the port name is invalid.

Action The port name for the individual port may contain 0–24 characters. Enter a name with 0–24 characters and re-submit. If spaces are used, enclose the name in quotation marks.

Message **Error 015: Invalid BB Credit**

Description The value entered for the buffer-to-buffer credit is invalid.

Action The buffer-to-buffer credit must be an integer in the valid range

Message **Error 016: Invalid R_A_TOV**

Description The value entered for the resource allocation time-out value is invalid.

Action The R_A_TOV is entered in tenths of a second and must be entered as an integer in the range 10–1200 (1 second to 120 seconds). The R_A_TOV value must be larger than the E_D_TOV value. Check to be sure that all conditions are met and re-submit.

Message **Error 017: Invalid E_D_TOV**

Description The value entered for the error detection time-out value is invalid.

Action The E_D_TOV is entered in tenths of a second and must be entered as an integer in the range 2–600 (0.2 second to 60 seconds). The E_D_TOV must be smaller than the R_A_TOV. Check to be sure that all conditions are met and re-submit.

Message **Error 018: Invalid TOV**

Description The E_D_TOV and R_A_TOV values are not compatible.

Action Enter a valid E_D_TOV / R_A_TOV combination. The E_D_TOV must be smaller than the R_A_TOV.

Message **Error 019: Invalid Operating Mode**

Description Informational Only.

Action Informational Only.

Message **Error 020: Invalid Preferred Domain ID**

Description The value entered for the preferred domain ID for the director or switch is invalid.

Action The preferred domain ID must be an integer in the range 1–31. Enter an appropriate value and re-submit.

Message **Error 021: Invalid Switch Priority**

Description The value entered for the switch priority is invalid.

Action The switch priority entered for the director or switch must be one of the following: principal, never principal, or default. Enter an appropriate value and re-submit.

Message **Error 022: Invalid Class 2 VC**

Description No longer used.

Action Informational Only

Message **Error 023: Invalid Class 3 VC**

Description No longer used.

Action Informational Only

Message **Error 024: Invalid Loop Class 2 VC**

Description No longer used.

Action Informational Only

Message **Error 025: Invalid Loop Class 3 VC**

Description No longer used.

Action Informational Only

Message **Error 026: Invalid Multicast VC**

Description No longer used.

Action Informational Only

Message **Error 027: VC Link Control**

Description No longer used.

Action Informational Only

Message **Error 028: VC Priorities**

Description No longer used.

Action Informational Only

Message **Error 029: Invalid Gateway Address**

Description The value entered for the gateway address is invalid.

Action The new gateway address for the Ethernet interface must be entered in dotted decimal format (e.g. 0.0.0.0). Enter an appropriate gateway address and re-submit.

Message **Error 030: Invalid IP Address**

Description The value entered for the IP Address is invalid.

Action The new IP address for the Ethernet interface must be entered in dotted decimal format (e.g. 10.0.0.0). Enter an appropriate IP address and re-submit.

Message **Error 031: Invalid Subnet Mask**

Description The value entered for the subnet mask is invalid.

Action The new subnet mask for the Ethernet interface must be entered in dotted decimal format (e.g. 255.0.0.0). Enter an appropriate subnet mask and re-submit.

Message **Error 032: Invalid SNMP Community Name**

Description The value entered for the SNMP community name is invalid

Action The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and re-submit.

Message **Error 033: Invalid SNMP Trap Address**

Description The value entered for the SNMP trap address is invalid.

Action The new SNMP trap address for the SNMP interface must be entered in dotted decimal format (e.g. 10.0.0.0). Enter an appropriate SNMP trap address and re-submit.

Message **Error 034: Duplicate Community Names Require Identical Write Authorization**

Description Two or more community names have been recognized as being identical, but their corresponding write authorizations are not identical.

Action Enter unique SNMP community names or force write authorizations for duplicate community names to be identical and re-submit.

Message **Error 035: Duplicate SNMP Trap Address**

Description The value entered for the SNMP trap address is already in use.

Action Enter a different SNMP trap address.

Message **Error 036: Port Already Swapped**

Description You tried to swap a port which is already in use. This message is only displayed when using the CLI interface.

Action Remove the port in use and the perform the action.

Message **Error 037: Invalid Month**

Description The value of the month entered for the new system date is invalid.

Action The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The month must contain an integer in the range 1–12. Enter an appropriate date and re-submit.

Message **Error 038: Invalid Day**

Description The value of the day entered for the new system date is invalid.

Action The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The day must contain an integer in the range 1–31. Enter an appropriate date and re-submit.

Message **Error 039: Invalid Year**

Description The value of the year entered for the new system date is invalid.

Action The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The year must contain an integer greater than 1980. Enter an appropriate date and re-submit.

Message **Error 040: Invalid Hour**

Description The value of the hour entered for the new system time is invalid.

Action The format of the time parameter must be hh:mm:ss. The hour can contain an integer in the range 0–23. Enter an appropriate time and re-submit.

Message **Error 041: Invalid Minute**

Description The value of the minute entered for the new system time is invalid.

Action The format of the time parameter must be hh:mm:ss. The minute can contain an integer in the range 0–59. Enter an appropriate time and re-submit.

Message **Error 042: Invalid Second**

Description The value of the second entered for the new system time is invalid.

Action The format of the time parameter must be hh:mm:ss. The second can contain an integer in the range 0–59. Enter an appropriate time and re-submit.

Message **Error 043: Invalid Statistics Group ID**

Description No longer used.

Action Informational Only

Message **Error 044: Max SNMP Communities Defined**

Description A new SNMP community may not be defined without removing an existing community from the list.

Action A total of 6 communities may be defined for SNMP. A new community can be added only after a current community is removed. Make the appropriate changes and re-submit.

Message **Error 045: Not Allowed While Switch Online**

Description The entered command requires that the director or switch be set offline.

Action Set the switch offline and re-submit the command.

Message **Error 046: Invalid Test Type**

Description Console server error.

Action Informational Only.

Message **Error 047: LIC Install Active**

Description Console server error.

Action Informational Only.

Message **Error 048: Invalid RADIUS Server Count Value**

Description An invalid value was entered for the number or retries or attempts.

Action Enter a valid value between 1 to 100.

Message **Error 049: Invalid RADIUS Server UDP Port Number**

Description An invalid value was entered.

Action Enter a valid RADIUS Server UDP Port Number; the default port number is 1812.

Message **Error 050: Invalid RADIUS Server Timeout Value**

Description An invalid value was entered.

Action Enter a valid RADIUS Server time-out value; the time-out value can be 1 to 1000 seconds; the default is 4 seconds.

Message **Error 051: Invalid RADIUS Server Transmit Attempts Value**

Description An invalid value was entered.

Action Enter a valid RADIUS Server time-out value; the value can be 1 to 100 attempts; default is 3 attempts.

Message **Error 052: Invalid RADIUS Server Deadtime Value**

Description An invalid value was entered.

Action Enter a valid RADIUS Server dead time value; the dead time may be 0 to 1440 minutes; default is 0.

Message **Error 053 Invalid RADIUS Key**

Description An invalid value was entered.

Action Enter a valid RADIUS Server key; this can be a key of 1-255 characters in length.

Message **Error 054 Buffer Limit Exceeded**

Description Internal error.

Action Informational Only.

Message	**Error 055: Invalid Zone Name**
Description	The value entered for the zone name is invalid.
Action	The zone name must be unique and contain 1–64 characters. The valid character set for the zone name can be found under *Creating and Modifying a Zone* on page 4-14. Make the appropriate changes to the zone name and re-submit.

Message	**Error 056: Undefined Zone**
Description	Zone name is missing.
Action	Enter a zone name.

Message	**Error 057: Duplicate Zone**
Description	Two or more zone names in the zone set are identical.
Action	All zone names must be unique. Make the appropriate changes and re-submit.

Message	**Error 058: Max Zones Defined**
Description	The maximum number of zones has already been defined.
Action	Delete a zone and then create a zone.

Message	**Error 059: Zone Name in Use**
Description	The zone name you entered is already in use.
Action	Enter a new zone name.

Message **Error 060: Invalid Number of Zone Members**

Description The entered command tried to add more zone members than the zone can hold.

Action Reduce the number of zone members in the zone and re-submit the command.

Message **Error 061: Invalid Zone Member Type**

Description A zone member was entered that is neither a WWN nor a Domain, Port pair.

Action Zone members must be expressed in WWN format or as a Domain, Port pair. Make the appropriate changes and re-submit.

Message **Error 062: Invalid Zone Set Name**

Description The value entered for the zone set name is invalid.

Action The zone set name must be contain 1–64 characters. Make the appropriate changes to the zone set name and re-submit.

Message **Error 063: Undefined Zone Set**

Description This message is displayed when a zone set has not been created.

Action Create a zone set.

Message **Error 064: Configuration changes have been limited to the API interface**

Description The API interface has restricted this interface from making configuration changes.

Action To make configuration changes from this interface, the API interface will need to update to allow this interface to make changes.

Message	**Error 065: Cannot remove the last CLI user with Administrators rights**
Description	There must be at least one administrator with access to the CLI.
Action	No action, you cannot remove the user account.

Message	**Error 066: Unknown Error**
Description	No longer used.
Action	Informational only.

Message	**Error 067: Invalid Number of Zone Set Members**
Description	You attempted to add another member to a zone set but the maximum number has been exceeded.
Action	Remove a zone member or do not add another zone member.

Message	**Error 068: The Switch IP Access Control List is Full**
Description	You attempted to add another member to the access control list but the list has reached the maximum number of members, or, the list being activated has an invalid number of IP pairs.
Action	Make sure there is at least one IP address in the Access Control List. Remove a zone member or do not add another zone member.

Message	**Error 069: Duplicate Port Name**
Description	Two or more port names are identical.
Action	Port names must be unique. Make appropriate changes and re-submit.

Message **Error 070: Invalid FRU Type**

Description The requested FRU does not exist on this product.

Action Consult the installation/service manual for this product to find appropriate FRU names.

Message **Error 071: FRU Not Installed**

Description The requested FRU is not installed.

Action Consult the installation/service manual for this product for appropriate action.

Message **Error 072: No Backup FRU**

Description The FRU swap cannot be performed because a backup FRU is not installed.

Action Insert a backup FRU and re-submit the request or consult the installation/service manual for this product for appropriate action.

Message **Error 073: Port Not Installed**

Description The port specified is not installed on this product.

Action Consult the installation/service manual on installing a port optic.

Message **Error 074: Invalid Number of Zones**

Description The specified zone set contains less than one zone or more than the maximum number of zones allowed for this product.

Action A zone set must contain at least one zone to be considered valid. Add or remove zones accordingly to meet specified requirements.

Message **Error 075: Invalid Zone Set Size**

Description The zone set entered exceeds switch NVRAM limitations.

Action Reduce the size of the zone set to meet specified requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.

Message **Error 076: Invalid Number of Unique Zone Members**

Description The zone entered contains more than the maximum number of zone members allowed per zone set for this product.

Action Reduce the number of members in one or more zones and re-submit the command.

Message **Error 077: Not Allowed While Port Is Failed**

Description The port selected is in a failed or inactive state, or is in need of service.

Action Consult the installation/service manual for appropriate action.

Message **Error 078: System Error Light On**

Description This unit is not able to beacon because the system error light is on.

Action You must clear the system error light before unit beaconing may be enabled. Consult the installation/service manual for appropriate action.

Message **Error 079: FRU Failed**

Description The specified FRU has failed.

Action Consult the installation/service manual for appropriate action.

Message **Error 080: Front Panel Failed**

Description No longer used.

Action Informational Only.

Message **Error 081: Default Zone Enabled**

Description The request cannot be completed because the default zone is enabled

Action Disable the default zone and re-submit the command.

Message **Error 082: Invalid Interop Mode**

Description The value entered for the interoperability mode is not valid.

Action The interoperability mode for the director or switch must be mcdata (McDATA Fabric 1.0) or open (Open Fabric 1.0). Make the appropriate changes and re-submit the command.

Message **Error 083: Not Allowed in Open Fabric Mode**

Description This request cannot be completed while this switch is operating in Open Fabric 1.0 mode.

Action Configure the interop mode to McDATA Fabric 1.0 mode.

Message **Error 084: Invalid Port PDCM**

Description FICON error message.

Action Informational Only.

Message **Error 085: Invalid Code Page**

Description FICON error message.

Action Informational Only.

Message **Error 086: Invalid Code Set**

Description FICON error message.

Action Informational Only.

Message **Error 087: Invalid GCSGID**

Description FICON error message.

Action Informational Only.

Message **Error 088: Invalid Feature Key Length**

Description The feature key installed is longer than the maximum length allowed.

Action Be sure that the key has been entered correctly and re-submit. Contact your sales representative with any further problems.

Message **Error 089: Not Allowed in FICON Style without SANtegrity Binding**

Description The SANtegrity feature is not installed.

Action Install the SANtegrity feature.

Message **Error 090: Invalid Port Type**

Description The port type configured is invalid.

Action A port may be configured to be an eport, gport, or fport. Be sure the port is configured appropriately and re-submit the command.

Message **Error 091: E_Port Type Configured**

Description Ports are not allowed to be configured as E_Ports in S/390 mode.

Action Configure the port as either a fport or gport and resubmit the command.

Message **Error 092: Not Allowed While Port Is Unblocked**

Description The port must be blocked to complete this request.

Action Block the port and re-submit the command.

Message **Error 093: Not Allowed While FICON MS Is Installed**

Description This request cannot be completed because FICON Management Server is installed.

Action This operation is not supported. No action necessary.

Message **Error 094: Invalid Feature Combination**

Description The features requested cannot be installed at the same time on one switch or director.

Action Contact your sales representative.

Message **Error 095: Invalid Switch Operating Mode**

Description Internal error.

Action Informational Only.

Message **Error 096: Invalid Chassis Serial Number**

Description Internal error.

Action Informational Only.

Message **Error 097: Invalid E-Port Capability**

Description Internal error.

Action Informational Only.

Message **Error 098: Chassis Serial Number is Zero**

Description No longer used.

Action Informational Only.

Message **Error 099: Preferred Domain ID Cannot Be Zero**

Description This product cannot be configured to have a preferred domain ID equal to zero (0).

Action Ensure that the ID is expressed as an integer in the range 1–31 and re-submit.

Message **Error 100: Port Binding Feature is Not Enabled**

Description You attempted to configure port binding but the feature is not enabled.

Action Enable the feature.

Message **Error 101: Command Not Supported on This Product**

Description This product does not support the requested command.

Action Command not supported. No action necessary.

Message **Error 102: Switch Not Operational**

Description The request cannot be completed because the switch is not operational.

Action Consult the installation/service manual and contact your service representative.

Message **Error 103: Port Diagnostic In Progress**

Description The request cannot be completed because a port diagnostic is running.

Action Wait for the diagnostic to complete.

Message **Error 104: System Diagnostic In Progress**

Description The request cannot be completed because a system diagnostic is running.

Action Wait for the diagnostic to complete.

Message **Error 105: Max Combination of Threshold Alert Definitions Reached**

Description The maximum number of total threshold alerts has already been reached.

Action Remove a threshold alert before adding the new threshold alert. A total of 16 counter and throughput threshold alerts is allowed.

Message **Error 106: Invalid Threshold Scope**

Description The scope of a threshold alert is not set to a valid state before the user activates an alert.

Action Set the scope of the threshold alert, then try to activate the alert.

Message **Error 107: Invalid Threshold State**

Description The state of a threshold alert must be set before the user activates an alert.

Action Set the state of the threshold alert, then try to activate the alert.

Message	**Error 108: Invalid TTA Type**
Description	The type of the throughput threshold alert has not been set.
Action	Set the type of the TTA, then try to activate the alert.

Message	**Error 109: Invalid CTA Type**
Description	The type of the counter threshold alert has not been set.
Action	Set the type of the CTA, then try to activate the alert.

Message	**Error 110: Invalid Percent Utilization**
Description	The type of the throughput threshold alert has not been set.
Action	Set the type of the TTA, then try to activate the alert.

Message	**Error 111: Invalid Threshold Type**
Description	The type of the threshold alert is not valid.
Action	Configure the type of the throughput threshold alert to one of the types found in the enumerated table for TTAs.

Message	**Error 112: No Threshold Definition Given**
Description	The threshold value for the alert was not configured before the user attempted to activate the alert.
Action	Set the threshold value, then try to activate the alert.

Message	**Error 113: Invalid EWS Enabled State**
Description	Internal error.
Action	Informational only.

Message **Error 114: Invalid CLI Enabled State**

Description Internal error.

Action Informational only.

Message **Error 115: Invalid Switch Speed**

Description The request cannot be completed because the switch is not capable of operating at the configured speed.

Action Consult the installation/service manual to determine the speed capabilities of your product.

Message **Error 116: Switch Not Capable of 2 Gb/sec**

Description The request cannot be completed because the switch is not capable of operating at 2 Gb/sec.

Action Consult the installation/service manual to determine the speed capabilities of your product.

Message **Error 117: Port Speeds Cannot be Set at Higher Data Rate than Switch Speed**

Description This request cannot be completed because the requested port speed is faster than the currently-configured switch speed.

Action The switch speed should first be configured to accommodate changes in the configured port speed. The ports cannot operate at a faster rate than the switch, itself. Update the switch speed and re-submit the request.

Message **Error 118: Invalid Port Speed**

Description This request cannot be completed because the requested port speed is not recognized for this product.

Action Port speeds may be set to 1 Gbps or 2 Gbps. Update the port speed and re-submit the request.

Message **Error 119: Switch Speed Not 2 Gb/sec**

Description This request cannot be completed because the switch speed has not been set to 2 Gb/s.

Action The switch speed must be set to 2 Gb/s in order to accommodate a port speed of 2 Gb/s. Update the switch speed and re-submit the request.

Message **Error 120: Invalid Trunking Enabled State**

Description Internal error.

Action Informational only.

Message **Error 121: Invalid Credit Starvation Threshold**

Description An invalid credit starvation threshold has been entered.

Action Submit the request with a valid value. The credit starvation threshold must be in the range of 1-99.

Message **Error 122: Invalid Port Congestion Threshold**

Description An invalid port congestion threshold has been entered.

Action Submit the request with a valid value. The port congestion threshold must be in the range of 1-99.

Message **Error 134: Invalid Membership List**

Description **Generic message to indicate a problem in either the switch binding or Fabric Binding Member list.**

Action Be sure that the membership list submitted does not isolate a switch already in the fabric. If this is not the case, the user needs to be aware of all fabric security rules and make sure that the list submitted adheres appropriately.

Message **Error 135: Invalid Number of Fabric Membership List Entries**

Description The number of fabric members submitted exceeds the maximum allowable entries of 31.

Action The number of entries in the fabric membership list is limited to the total number of domain ID's available to the fabric. Make sure that the list (including the managed switch) contains no more than 31 entries.

Message **Error 136: Invalid Number of Switch Binding Membership List Entries**

Description The number of switch members submitted exceeds the maximum allowable entries of 256.

Action The number of entries in the Switch Binding Membership List is limited to 256. Make sure that the list (including the managed switch) contains no more than 256 entries.

Message **Error 137: Invalid Fabric Binding State**

Description The fabric binding state submitted is not recognized.

Action The fabric binding state must be set to either “inactive” or “restrict.”

Message **Error 138: Invalid Switch Binding State**

Description The switch binding state submitted is not recognized.

Action The switch binding state must be set to one of the following: 'Enabled, Restrict E Ports', 'Enabled, Restrict F Ports', 'Enabled, Restrict All Ports', or 'Disabled'.

Message **Error 139: Insistent Domain ID's Must Be Enabled When Fabric Binding Active**

Description The user attempted to disable insistent domain ID's while fabric binding was active.

Action Insistent domain ID's must remain enabled while fabric binding is active. If fabric binding is set to inactive, the insistent domain ID state may be changed. It should be noted, however, that this can be disruptive to the fabric.

Message **Error 140: Invalid Insistent Domain ID State**

Description The request cannot be completed because an invalid insistent domain ID state has been submitted.

Action The insistent domain ID state must be set to either *enable* or *disable*.

Message **Error 141: Invalid Enterprise Fabric Mode**

Description The request cannot be completed because an invalid enterprise fabric mode has been submitted.

Action The enterprise fabric mode must be set to either *enable* or *disable*.

Message **Error 142: Invalid Domain RSCN State**

Description The request cannot be completed because an invalid domain RSCN state has been submitted.

Action The domain RSCN state must be set to either *enable* or *disable*.

Message **Error 143: Domain RSCNs Must Be Enabled When Enterprise Fabric Mode Active**

Description The user attempted to disable domain RSCN's while enterprise fabric mode was active.

Action Domain RSCN's must remain enabled while the enterprise fabric mode is active. If enterprise fabric mode is set to inactive, the domain

RSCN state may be changed. It should be noted, however, that this can be disruptive to the fabric.

Message **Error 144: The SANtegrity Feature Has Not Been Installed**

Description The user attempted to activate a change to the fabric security configuration without first installing the SANtegrity feature key.

Action If this key has not been installed, contact your sales representative.

Message **Error 146: Fabric Binding May Not Be Deactivated While Enterprise Fabric Mode Active**

Description The user attempted to deactivate fabric binding while enterprise fabric mode was active.

Action Fabric binding must be active while operating in enterprise fabric mode. The fabric binding state may be changed if enterprise fabric mode is deactivated. It should be noted, however, that this can be disruptive to the fabric.

Message **Error 148: Not Allowed While Switch Offline**

Description The switch must be online to complete this request.

Action Change the state of the switch to ONLINE and re-submit the request.

Message **Error 149: Not Allowed While Enterprise Fabric Mode Active and Switch Online**

Description The request cannot be completed while the switch is online and enterprise fabric mode is Active.

Action This operation will be valid if the switch state is set to offline and enterprise fabric mode to inactive. It should be noted, however, that this can be disruptive to the fabric.

Message **Error 151: Invalid Open Systems Management Server State**

Description The request cannot be completed because the OSMS state submitted is invalid.

Action The OSMS state may be set to either *enable* or *disable*.

Message **Error 152: Invalid FICON Management Server State**

Description The request cannot be completed because the FICON MS state submitted is invalid.

Action The FICON MS state may be set to either *enable* or *disable*.

Message **Error 153: Feature Key Not Installed**

Description The request cannot be completed because the required feature key has not been installed to the firmware.

Action Contact your sales representative.

Message **Error 154: Invalid Membership List WWN**

Description The request cannot be completed because the WWN does not exist in the switch binding membership list.

Action Make sure that the WWN deleted matches the WWN in the Switch Binding Membership List. Make appropriate changes and re-submit the request.

Message **Error 155: Cannot Remove Active Member From List**

Description This member cannot be removed from the fabric security list because it is currently logged in.

Action Fabric security rules prohibit any device or switch from being isolated from the fabric via a membership list change. If it is truly the intention of the user to remove the device in question from the membership list, then there are several approaches to take. This request may be completed most non-disruptively by blocking the

port (or physically removing the device from the managed switch) to which this device is attached and resubmitting the request.

Message **Error 156: Cannot Complete While Switch is Online and Fabric Binding Active**

Description The switch must be offline and Fabric Binding must be inactive before this feature can be disabled.

Action Deactivating this feature can be disruptive to Fabric operations. Take the switch offline and make sure deactivate fabric binding before disabling this feature.

Message **Error 158: Invalid Switch IP Access Control List IP Address Range**

Description The pair of IP addresses are invalid and cannot be added to the list.

Action Make sure the IP addresses are valid and the first IP is lower than the second.

Message **Error 159: Invalid IP Access Control List Pairs Count Value**

Description The list being activated has an invalid number of IP pairs.

Action Make sure there is at least one IP address in the Access Control List.

Message **Error 160: Management Client IP Not Included In IP Access Control List**

Description The management interface IP address is not in the list.

Action The management IP must be in the list or the current connection would be lost.

Message **Error 161: The Switch IP Access Control List is Empty**

Description The management interface IP address is not in the list.

Action The management IP must be in the list or the current connection would be lost.

Message **Error 162: List is full**

Description There is no more room for new entries in the list.

Action Remove a different entry and try again.

Message **Error 163: FICON MS feature key must be installed**

Description The command is not available without the FICON MS feature key.

Action Install the FICON MS feature key.

Message **Error 164: FICON CUP Zoning feature key must be uninstalled**

Description The operation cannot be completed with the FICON CUP Zoning key installed.

Action Remove the FICON CUP Zoning feature key.

Message **Error 165: CUP Zoning feature key must be installed**

Description The command is not available without the FICON CUP Zoning feature key.

Action Install the FICON CUP zoning feature key.

Message **Error 166: CUP Zoning feature must be enabled**

Description The command cannot be completed with the CUP Zoning feature disabled.

Action Enable FICON CUP Zoning.

Message **Error 167: Diagnostics can not be run on inactive port**

Description The port is in the inactive state and diagnostics can't be run.

Action The port state must change out of the inactive state.

Message **Error 168: Duplicate member in the list**

Description The member is already in the list.

Action Duplicate members are not allowed in the list.

Message **Error 169: Cannot enable CNT feature**

Description CNT support is in the wrong state.

Action The enabled state for CNT support must be changed.

Message **Error 170: Duplicate IP Address pair in the Access Control List**

Description Duplicate IP address pairs are not allowed in the Access Control List.

Action This command is redundant, the member already exists in the list.

Message **Error 171: Invalid username**

Description The username is invalid.

Action Enter a unique username using only the allowed characters and proper length.

Message **Error 172: Invalid list size**

Description The number of entries in the list is invalid.

Action Make sure the list has at least one entry.

Message	**Error 173: Invalid value**
Description	The value being entered is invalid.
Action	Enter a valid value.

Message	**Error 174: Invalid list data**
Description	The list data is invalid.
Action	Correct the list to make it a valid list.

Message	**Error 175: Invalid list index**
Description	The list data is invalid.
Action	Correct the list to make it a valid list.

Message	**Error 176: Entry not found in the list**
Description	The desired entry in the list does not exist.
Action	Make sure the desired entry is in the list and it is being typed correctly.

Message	**Error 177: Cannot remove the last user with Administrator rights**
Description	At least one Administrator user must exist for each management interface.
Action	Add a new Administrator and then try again.

Message	**Error 178: Invalid password**
Description	The entered password is invalid.
Action	Enter a password using valid characters and a proper length.

Message **Error 179: Insistent Domain IDs must be enabled**

Description To complete this command, Insistent Domain IDs must be enabled.

Action Enabled Insistent Domain IDs.

Message **Error 180: Too many management interface users**

Description Only 25 management users can be added to the user database.

Action Remove other management users in order to make room for a new one.

Message **Error 181: Preferred path must be disabled**

Description The Preferred Path feature must be disabled.

Action Disable the Preferred Path feature.

Message **Error 182: Source port must be different than the exit port**

Description The source and exit ports cannot be the same.

Action Configure a preferred path with different source and exit ports.

Message **Error 183: Invalid Fencing Policy State**

Description The enable status is invalid

Action Enter a valid enable status

Message **Error 184: Invalid Fencing Policy Time Period**

Description The entered period is invalid

Action Enter a valid period

Message	**Error 185: Invalid Limit Value for this Fencing Policy Type**
Description	The entered limit is invalid
Action	Enter a valid limit

Message	**Error 186: Cannot Block this Port**
Description	Port is not blockable
Action	Enter a valid port number

Message	**Error 187: cannot beacon this port**
Description	Cannot enable beaconing on this port
Action	Enter a valid port number

Message	**Error 188: Port Swap Classification is Not Identical**
Description	Cannot swap ports because the port swap classification is not identical.
Action	Swap different ports or install a FRU with the same port classification.

Message	**Error 189: invalid fencing policy type**
Description	Invalid fencing policy type
Action	Enter a valid fencing policy type

Message	**Error 190: invalid fencing policy port type**
Description	Invalid fencing policy port type
Action	Enter a valid port or port type

Message **Error 191: max fencing policy definitions reached**

Description A new port fencing policy may not be defined without removing an existing port fencing policy from the list.

Action A total of 14 policies may be defined for port fencing. A new policy can be added only after a current policy is removed; make the appropriate changes and re-submit.

Message **Error 192: Invalid Fencing Policy Name**

Description Port fencing name is invalid

Action Configure a valid port fencing name.

Message **Error 193: Cannot Modify an Enabled Fencing Policy**

Description The policy cannot be modified while it is enabled

Action Disabled the policy before modifying

Message **Error 194: Cannot enable two policies of the same type that contain the same ports**

Description Two policies of the same type cannot be enabled if they have ports that are in both lists.

Action Make sure the policy that is being enabled does not have the same port number as a policy that is already enabled

Message **Error 195: Cannot enable two policies of the same type that contain same port scope**

Description Two policies of the same type cannot be enabled if they have the same port type.

Action Make sure the policy that is being enabled does not have the same port type as a policy that is enabled.

Message	**Error 196: Cannot enable two policies of the same type that contain default scope**
Description	Two policies of the same type cannot be enabled if both policies use the default ports.
Action	Only enable one policy that is using the default ports.

Message	**Error 197: Port list contains no ports**
Description	The policy port list must contain ports or a port scope
Action	Add ports or a port scope to the policy

Message	**Error 198: Duplicate Authentication Name**
Description	Authentication names must be unique
Action	Configure a unique authentication name

Message	**Error 199: Unknown Error**
Description	The error cannot be diagnosed.
Action	Informational only.

Message	**Error 200: Success**
Description	The action was completed successfully.
Action	Informational only.

Message	**Error 201: Change Authorization Request Failed**
Description	The switch did not accept the request to make a change to NVRAM.
Action	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.

Message **Error 202: Invalid Change Authorization ID**

Description The switch will not accept a change request from this particular client.

Action Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.

Message **Error 203: Another Client Has Change Authorization**

Description Another user is currently making changes to this switch.

Action Be sure all parameters have been entered correctly and re-submit.

Message **Error 207: Change Request Failed**

Description The switch did not accept the request.

Action Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.

Message **Error 208: Change Request Timed Out**

Description Authorization time to make NVRAM changes has expired.

Action Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.

Message **Error 209: Change Request Aborted**

Description The switch did not accept the request.

Action Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.

Message **Error 210: Busy Processing Another Request**

Description A different switch in the Fabric was busy processing another request and could not complete the command.

Action Be sure all parameters have been entered correctly and re-submit. Contact your service representative with continued problems.

Message **Error 211: Duplicate Zone**

Description Two or more zone names in the local zone set are identical.

Action All zone names must be unique. Make the appropriate changes and re-submit.

Message **Error 212: Duplicate Zone Member**

Description A member was added that already exists in the zone.

Action No action necessary.

Message **Error 213: Number of Zones Is Zero**

Description You are attempting to activate and empty zone set.

Action The zone set must have at least one zone to be considered valid. Add a valid zone to the zone set and re-submit.

Message **Error 214: A Zone Contains Zero Members**

Description You are attempting to activate a zone set that contains at least one zone with zero members.

Action Each zone in the zone set must contain at least one member. Add a valid member to the empty zone and re-submit.

Message **Error 215: Zone Set Size Exceeded**

Description The local work area zone set has outgrown the size limitations imposed by the Command Line Interface.

Action Reduce the size of the zone set to meet requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.

Message **Error 216: No Attached Nodes Exist**

Description There are no attached nodes.

Action To add more members, attach more devices to the switch or add the members by WWN or Domain ID and port.

Message **Error 217: All Attached Nodes are in the Zone**

Description All the attached nodes are already in use.

Action To add more members, attach more devices to the switch or add the members by WWN or Domain ID and port.

Message **Error 218: Invalid Port Number**

Description The value entered for the port number is invalid

Action Enter a port number within the range supported by your director or switch.

Message **Error 219: Invalid Port Type**

Description The port type configured is invalid.

Action A port may be configured to be an eport, gport, or fport. Be sure the port is configured appropriately and re-submit the command. On the 12-port and 24-port switches only, fxport and gxport types are also supported. On the 12-port switch, the Fabric Capable feature must be installed to configure a E_Port, G_Port, or Gx_Port.

Message	**Error 220: Cannot Run Diagnostics While a Device is Logged into the Port**
Description	Diagnostics cannot be run while a device is logged into the port.
Action	Block the port to run diagnostics.

Message	**Error 221: Cannot Run Diagnostics on an Active E-Port**
Description	Diagnostics cannot be run on an active E-Port.
Action	Block the port to run diagnostics.

Message	**Error 222: Invalid SNMP Community Index**
Description	The value entered for the SNMP community index is invalid.
Action	The SNMP community index must be an integer in the range 1–6. Make the appropriate changes and re-submit the command.

Message	**Error 223: Unknown Error**
Description	The switch did not accept the request
Action	Contact your service representative.

Message	**Error 224: Invalid Argument**
Description	One or more parameters are invalid for this command.
Action	Consult this manual or appropriate parameter names. Parameters must be typed exactly to specification to be recognized correctly.

Message	**Error 225: Argument Does Not Contain all USASCII Characters**
Description	One or more parameters are invalid for this command.

Action Enter only ASCII characters.

Message **Error 226: Argument Is Too Long**

Description One or more parameters are invalid for this command.

Action For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly.

Message **Error 227: Invalid SNMP Community Name**

Description The value entered for the SNMP community name is invalid

Action The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and re-submit.

Message **Error 228: Invalid Write Authorization Argument**

Description The writeAuthorization parameter does not contain a valid value.

Action Parameters must be typed exactly to specification to be recognized correctly.

Message **Error 229: Invalid UDP Port Number**

Description The udpPortNum parameter does not contain a valid value.

Action Parameters must be typed exactly to specification to be recognized correctly.

Message **Error 230: Invalid WWN**

Description The wwn parameter does not contain a valid value.

Action For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly.

Message **Error 231: Invalid Port number**

Description The portNum parameter does not contain a valid value.

Action For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly.

Message **Error 232: Invalid Domain ID**

Description The domainID parameter does not contain a valid value.

Action For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly.

Message **Error 233: Invalid Member**

Description The zone member added is not valid.

Action For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly.

Message **Error 234: Invalid Command**

Description The system cannot associate an action with the submitted command. The command may be misspelled, required parameters may be missing, or the request may not be applicable to the branch of the CLI tree from which it was submitted.

Action Consult the documentation for the command to be sure this command was entered correctly, all parameters are valid and present, and that the syntax is correct.

Message **Error 235: Unrecognized Command**

Description The CLI does not recognize the command and cannot perform the help '?' command as requested.

Action The entered command is misspelled or the prompt is not positioned at the right place in the CLI command tree for this command. For the appropriate syntax, see the section of the manual that corresponds to the attempted command.

Message **Error 236: Ambiguous Command**

Description The CLI does not recognize the command issued.

Action The CLI cannot interpret the command because a unique match cannot be identified. For the appropriate syntax, see the section of the manual that corresponds to the attempted command. Enter the complete command and re-submit.

Message **Error 237: Invalid Zoning Database**

Description There was an unidentifiable problem in the local zone set work area.

Action Verify all parameters are entered correctly and re-submit. Otherwise, the pending zone set should be cleared and reconstructed.

Message **Error 238: Invalid Feature Key**

Description The feature key entered is invalid.

Action Verify that the feature key was entered correctly and re-submit. Contact your service representative with further difficulties.

Message **Error 239: Fabric binding entry not found**

Description The user requested to remove a fabric binding entry that is not in the pending fabric membership list.

Action Verify that the correct entry (both WWN and Domain ID) is being requested for removal from the list and re-submit the request.

Message **Error 240: Duplicate fabric binding member**

Description The user requested to add an entry to the fabric binding list that is already a member of the list.

Action Verify that the correct entry (both WWN and Domain ID) is being requested for addition to the list and re-submit the request.

Message **Error 241: Comma-delimited mode must be active**

Description Comma-delimited mode must be active to execute this command

Action Some commands require that comma-delimited mode be active (e.g. show.nameserverExt). Enable comma-delimited mode and re-issue the command.

Message **Error 242: Open trunking threshold % value must be 1–99**

Description An invalid threshold percentage has been entered.

Action The Open trunking threshold must be in the range 1–99. Make sure all values are valid and re-submit the request.

Message **Error 244: Not allowed while Enterprise Fabric Mode is Active and Switch is Online**

Description This operation is not allowed while the switch is in Enterprise Fabric Mode and the switch is Online.

Action Make sure Enterprise Fabric Mode is not enabled and the switch is offline.

Message **Error 245: Invalid increment value**

Description The increment value specified is not between 1 and 70560.

Action Make sure the increment value given is between 1 and 70560.

Message **Error 246: Invalid interval value**

Description The interval value specified is not between 5 and 70560 minutes.

Action Make sure the increment value given is between 5 and 70560 minutes.

Message **Error 247: Invalid counter number**

Description The counter specified is not a valid number.

Action Use the table output by the command perf.counterThreshAlerts.showStatisticsTable to find a valid counter value.

Message **Error 248: A counter must be assigned to this threshold alert**

Description A counter must be assigned to an alert before it is enabled.

Action Use the perf.counterThreshAlerts.setCounter command to set a counter before the alert is enabled.

Message **Error 249: At least one port or port type must be added to this threshold alert**

Description A port or port type must be assigned to an alert before it is enabled.

Action Use the perf.counterThreshAlerts.addPort command to add a port before the alert is enabled.

Message **Error 250: Invalid counter threshold alert name**

Description The name specified for the alert is not valid.

Action Specify a counter threshold alert name that has already been created.

Message	**Error 251: The threshold alert must be disabled**
Description	The counter threshold alert to be modified/deleted is already enabled.
Action	Disable the threshold alert and then try the command again.

Message	**Error 253: Cannot Remove a Member Currently Interacting with the Fabric**
Description	Current members of the fabric must be included in the Fabric Binding List.
Action	Do not remove active fabric members from the pending Fabric Binding Member List.

Message	**Error 254: A utilization type must be assigned to this threshold alert**
Description	A utilization type must be set before activating this threshold alert.
Action	Add a utilization type and then the threshold alert can be activated.

Message	**Error 255: Invalid throughput threshold alert name**
Description	The name of the threshold alert is incorrect.
Action	Either the name does not exist, or the new name cannot be used because it is illegal or a duplicate.

Message	**Error 256: Invalid utilization type number**
Description	The utilization type number does not exist.
Action	Select a valid utilization type number.

Message	**Error 257: Invalid utilization percentage value**
Description	The utilization percentage value is out of range.

Action Select a valid utilization percentage value.

Message **Error 258: Invalid duration value**

Description The duration value in minutes is out of range.

Action Select a valid duration value.

Message **Error 259: Invalid threshold alert name**

Description The name of the threshold alert is incorrect.

Action The threshold alert name does not exist.

Message **Error 260: Not Allowed while SANtegrity feature is not installed on remote switch**

Description All switches in the fabric must have the SANtegrity feature key installed.

Action Install the SANtegrity feature key on all switches in the fabric.

Message **Error 261: No Attached Members Exist**

Description There are no members attached to the switch.

Action Check all connections and make sure attached devices are present

Message **Error 262: All Attached Members are in the Membership List**

Description All attached fabric members are already in the membership list.

Action This action is redundant, all members are already in the list.

Message	**Error 263: The SANtegrity Authentication feature key is not installed**
Description	The SANtegrity Authentication feature key is not installed.
Action	Install the SANtegrity Authentication feature key.

Message	**Error 264: The Preferred Path feature key is not installed**
Description	The preferred path feature key must be installed.
Action	Install the preferred path feature key.

Message	**Error 265: Duplicate threshold alert name**
Description	The desired name for the threshold alert is already in use.
Action	Use a different name for the threshold alert.

Message	**Error 266: Attached members cannot be added while fabric is building**
Description	Attached members cannot be added while the fabric is building.
Action	The fabric is still building, wait a couple of seconds until it is complete.

Message	**Error 267: RADIUS server IP Address is Too Long**
Description	The IP address was entered incorrectly or is too long.
Action	Enter the correct IP address.

Message	**Error 268: RADIUS key too long**
Description	The RADIUS key you entered is too long.
Action	Enter a shorter RADIUS key

Message	**Error 269: Invalid retransmit attempts. Must be between 1 and 100**
Description	The desired retransmit attempt value is invalid
Action	Select a retransmit value between 1 and 100

Message	**Error 270: Invalid timeout value. Must be between 1 and 1000**
Description	The desired timeout value is invalid
Action	Select a timeout value between 1 and 10000

Message	**Error 271: Invalid deadtime value. Must be between 0 and 1440 minutes**
Description	The desired deadtime value is invalid
Action	Select a deadtime value between 0 and 1440

Message	**Error 272: Invalid host name and port combination**
Description	The desired host name and port combination does note exist in the database or is invalid
Action	Select a valid host name and port combination

Message	**Error 273: Passwords do not match**
Description	The password does not match the confirm password
Action	Re-enter the command and enter matching passwords

Message	**Error 274: Invalid interface combination**
Description	The desired interface is not a valid interface
Action	Select a valid interface value

Message	**Error 275: Invalid authentication role**
Description	The desired role is not a valid role
Action	Select a valid role. Valid roles are administrator, operator, or no role.

Message	**Error 276: Invalid sequence authentication combination**
Description	The desired sequence is not a valid sequence
Action	Select a valid sequence. Valid sequences are *Local Only, RADIUS Only,* and *RADIUS then Local*.

Message	**Error 277: Roles cannot be assigned to a username with this interface**
Description	The role of the selected username is not configurable.
Action	This operation is not supported. No action necessary.

Message	**Error 278: CHAP authenticated passwords must be exactly 16 bytes**
Description	The CHAP authentication password must be exactly 16 bytes
Action	Enter a CHAP authentication password that is exactly 16 bytes

Message	**Error 279: Must Specify a RADIUS Key**
Description	You performed an action that requires a RADIUS key.
Action	Enter the correct RADIUS key.

Message	**Error 280: Zone Member does not exist**
Description	The desired zone member does not exist
Action	Select a valid zone member

Message **Error 281: Zone does not exist**

Description The desired zone does not exist

Action Select a valid zone name

Message **Error 282: Conflicting Domain ID for the specified WWN**

Description The desired Domain ID is already in use

Action Select a different Domain ID

Message **Error 283: Conflicting WWN for the specified Domain ID**

Description The WWN is already in use

Action Select a different WWN

Message **Error 284: FICON CUP Zoning host control list is full**

Description A new host may not be entered without removing an existing host from the list

Action A total of eight hosts may be defined for the FICON CUP Zoning host control list. A new host can be added only after a current host is removed. Make the appropriate changes and re-submit

Message **Error 285: WWN not found in host control list**

Description The desired WWN is not in the host control list

Action Select a WWN that is in the host control list

Message **Error 286: Invalid Number of NPIV Allowed Logins**

Description The number of login attempts exceeded the maximum allowable number.

Action Select a value between 1 and 256.

Message **Error 287: Port is unaddressable**

Description The desired port cannot be configured because it is unadressable

Action This operation is not supported. No action necessary.

Message **Error 288: The NPIV feature key must be installed.**

Description An attempt was to access feature was accessed that has not been installed

Action Install the feature key.

Message **Error 289: Duplicate policy name**

Description A policy cannot be added if it has the same name as an existing policy

Action Select a different policy name

Message **Error 290: No Optic Installed**

Description There is not an optic in the port for the specified port number

Action Select a different port number, or plug in an optic

Message **Error 291: Port Inaccessible**

Description The port is inaccessible for the given port number

Action Select a different port number

Message **Error 292: Port Number out of Range**

Description The specified port number is out of range for the given product.

Action Select a different port number

Message **293: Cannot modify users with default passwords**

Description No longer used.

Action None.

Message **294: Invalid RADIUS Index**

Description The specified RADIUS index is invalid.

Action Enter a valid index; valid indexes are 1 to 3.

Message **295: Invalid MIHPTO Value**

Description The MIHPTO value was invalid. This message is only displayed with the CLI interface.

Action Enter a valid MIHPTO value.

Message **296: Cannot Delete the Last E-port User with Authentication Setting**

Description There must be at least one administrator with access to the E-port interface.

Action No action, you cannot remove the user account.

Message **297: Cannot Delete the Last N-Port User with Authentication Setting**

Description There must be at least one administrator with access to the N-port interface.

Action No action, you cannot remove the user account.

Message **298: Cannot Delete the Last API User with Authentication Setting**

Description There must be at least one administrator with access to the API interface.

Action No action, you cannot remove the user account.

Message **299: CHAP Secret Not Defined**

Description The CHAP secret must be defined for Open Systems Management Server before enabling outgoing authentication.

Action Define a CHAP secret for Open Systems Management Server.

Message **300: No User Defined for this Interface**

Description You cannot perform this action unless a user (account) is defined for the interface.

Action Create a user account for the interface.

Message **301: RADIUS Server Undefined**

Description You cannot perform this operation until a RADIUS server is configured. (You cannot enable RADIUS authentication if there is not a RADIUS server already configured.)

Action Configure a RADIUS server before enabling RADIUS authentication.

Message **302: Pending Default Zone Member Count Exceeds Threshold**

Description You cannot enable default zoning if the there are more than 64 devices which are not included in a zone (unzoned).

Action Reduce the number of devices that are not included in a zone (unzoned).

Message **303: Invalid Preferred Path**

Description The preferred path is invalid; one reason may be that the Domain ID is the same as the local switch ID.

Action Enter a valid preferred path and ensure the Domain ID is not the same as the local switch ID.

Message **304: RADIUS Authentication Present. Cannot Remove All RADIUS Servers.**

Description You cannot remove all of the RADIUS server configurations if you have enabled RADIUS authentication.

Action Disable RADIUS authentication on all interfaces (such as CLI and so on) and then remove the last RADIUS server.

Message **305: OSMS Management State must be Enabled.**

Description You cannot enable CT Outgoing Authentication when Open Systems Management Server is disabled.

Action Enabled Open Systems Management Server before enabling CT Outgoing Authentication.

Message **306: CT Outgoing Authentication is Enabled.**

Description You cannot disable Open Systems Management Server when CT outgoing authentication is enabled.

Action Disable CT outgoing authentication before disabling Open Systems Management Server.

Message **307: The Preferred Path Does Not Exist.**

Description You tried to clear a path that does not exist.

Action Verify the path you attempted to clear exists.

Message **308: Invalid Line Speed Combination.**

Description The Ethernet speed/duplex combination is invalid.

Action Enter a valid Ethernet speed/duplex combination.

Message **Error 310: FICON Management Server must be enabled**

Description You cannot perform this operation until the FICON Management Server is enabled.

Action Enable the FICON Management Server.

Message **Error 311: FICON CUP Zoning must be disabled**

Description You cannot perform this operation until the FICON Management Server is disabled.

Action Disable the FICON Management Server.

Message **Error 321: Invalid syslog facility number**

Description The syslog facility number is invalid

Action Select a valid syslog facility number.

Message **Error 323: Invalid trigger start offset**

Description The trigger start offset value is invalid.

Action Select a valid trigger start offset value.

Message **Error 324: Invalid trigger start bit pattern**

Description The trigger start bit pattern is invalid.

Action Select a valid trigger start bit pattern.

Message **Error 325: Invalid trigger end offset**

Description The trigger end offset value is invalid.

Action Select a valid trigger end offset value.

Message **Error 326: Invalid trigger end bit pattern**

Description The trigger end bit pattern is invalid.

Action Select a valid trigger end bit pattern.

Message **Error 327: Invalid trigger**

Description The trigger is invalid.

Action Enter a valid trigger value.

Message **Error 328: Invalid syslog index**

Description The syslog index is invalid.

Action Select a valid syslog index.

Message **Error 330: Invalid trace route source**

Description The trace route source value is invalid.

Action Select a valid WWN or Port ID for the trace route source.

Message **Error 331: Invalid trace route destination**

Description The trace route destination value is invalid.

Action Select a valid WWN or Port ID for the trace route destination.

Message	**Error 332: Unable to run a trace route at this time**
Description	The trace route is unable to run.
Action	Wait a little while and run the trace route again.

Message	**Error 333: Invalid Port ID**
Description	The Port ID is invalid.
Action	Enter a valid Port ID.

Message	**Error 336: Invalid SSL renegotiation megabyte value**
Description	The SSL renegotiation megabyte value is invalid
Action	Enter a valid SSL renegotiation megabyte value

Message	**Error 337: Invalid SNMP table index**
Description	The SNMP table index is invalid
Action	Select a valid index.

Message	**Error 339: Invalid SNMPv3 user table index**
Description	The user table index is invalid.
Action	Enter a valid index.

Message	**Error 340: Invalid SNMPv3 username**
Description	The username is invalid.
Action	Select a valid username.

Message **Error 341: Invalid SNMPv3 authentication protocol**

Description The authentication protocol is invalid.

Action Select a valid authentication protocol.

Message **Error 342: Invalid SNMPv3 authentication key**

Description The authentication key is invalid.

Action Select a valid authentication key.

Message **Error 343: Invalid SNMPv3 privacy protocol**

Description The privacy protocol is invalid.

Action Select a valid privacy protocol.

Message **Error 344: Invalid SNMPv3 privacy key**

Description The privacy key is invalid.

Action Select a valid privacy key.

Message **Error 345: Invalid SNMPv3 target table index**

Description The target table index is invalid.

Action Select a valid index.

Message **Error 346: Invalid SNMPv3 target IP**

Description The Target IP Address is invalid.

Action Enter a valid IP Address.

Message	**Error 347: Invalid SNMPv3 UDP port number**
Description	The UDP Port number is invalid.
Action	Select a valid UDP port number.

Message	**Error 348: Invalid SNMPv3 community name**
Description	The community name is invalid.
Action	Enter a valid community name.

Message	**Error 349: Invalid SNMPv3 MP model**
Description	The MP model is invalid.
Action	Enter a valid MP model.

Message	**Error 350: Invalid SNMPv3 security name**
Description	The security name is invalid.
Action	Enter a valid security name.

Message	**Error 351: Invalid SNMPv3 group name**
Description	The group name is invalid.
Action	Enter a valid group name.

Message	**Error 352: Invalid SNMPv3 security model**
Description	The security model is invalid.
Action	Enter a valid security model.

Message **Error 353: Invalid SNMPv3 security level**

Description The security level is invalid.

Action Enter a valid security level.

Message **Error 354: Invalid SNMPv3 access table index**

Description The access table index is invalid.

Action Enter a valid index.

Message **Error 360: The number of days for key generation is out of range.**

Description The number of days for the key generation is invalid.

Action Enter a valid number of days for key generation.

Message **Error 361: An internal error occurred when generating the key.**

Description An error occurred while generating the SSL key.

Action None

Message **Error 362: Duplicate SNMPv3 user name**

Description You can't have two SNMPv3 usernames that are the same.

Action Enter a different value for the username.

Message **Error 363: Invalid SNMPv3 group table index**

Description The group table index is invalid.

Action Enter a valid index.

Message **Error 364: SNMPv3 group name conflict**

Description The group name, security name, security model combination must be unique.

Action Enter a valid group name, security name, and security model combination.

Message **Error 367: Invalid SNMPv3 access group name**

Description The access group name is invalid.

Action Enter a valid access group name.

Message **Error 371: Unable to set HA mode**

Description The HA mode cannot be set.

Action Contact your service representative.

Message **Error 372: The IP ACL pair does not exist in the Switch Access Control List**

Description The IP ACL pair is already not in the list.

Action None

Message **Error 373: Configuration not allowed while SNMPv3 is enabled**

Description You can't perform the desired operation while SNMPv3 is enabled.

Action Disable SNMPv3 before continuing.

Message **Error 374: Invalid SNMPv3 securitytogroup index**

Description The security to group table index is invalid.

Action Enter a valid index.

Message **Error 376: The Local Switch WWN or DID conflicts with another member**

Description There is a member in the FBML that has the same WWN or DID as the local switch.

Action Remove the conflicting entry and then add the local switch to the list.

Message **Error 377: HA Mode cannot be turned off with both Power Supply connected**

Description When both power supplies are connected, the HA Mode cannot be disabled.

Action None

Message **Error 378: Duplicate IP address**

Description The IP address already exists.

Action Choose a different IP Address or remove the existing entry.

Glossary

This glossary includes terms and definitions from:

- *American National Standard Dictionary for Information Systems* (ANSI X3.172-1990), copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 25 West 42nd Street, New York, NY 10036. Definitions from this text are identified by *(A).*
- *ANSI/EIA Standard - 440A: Fiber Optic Terminology*, copyright 1989 by the Electronic Industries Association (EIA). Copies can be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue N.W., Washington, D.C. 20006. Definitions from this text are identified by *(E).*
- *IBM Dictionary of Computing* (ZC20-1699). Definitions from this text are identified by *(D).*
- *Information Technology Vocabulary*, developed by Subcommittee 1 (SC1), Joint Technical Committee 1 (JTC1), of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Definitions of published parts of this vocabulary are identified by *(I).* Definitions taken from draft international standards, committee drafts, and working papers developed by ISO/IEC SC1/JTC1 are identified by *(T),* indicating that final agreement has not been reached among the participating national bodies of SC1.

A

access The ability and means necessary to store data in, to retrieve data from, to transfer data into, to communicate with, or to make use of any resource of a storage device, a system, or area such as random access memory (RAM) or a register.

access control A list of all devices that can access other devices across the network and the permissions associated with that access. *See also* persistent binding; zoning.

active configuration In FICON management style, the director or switch configuration that is determined by the status of the connectivity attributes.

active FBML The active Fabric Binding Member list. When fabric binding is active, the list of fabric members with which the product is allowed to communicate. *See* fabric binding and Fabric Binding Member List.

active field-replaceable unit Active FRU. A FRU that is currently operating as the active, and not the backup FRU. *See also* backup field-replaceable unit.

active FRU *See* active field-replaceable unit.

active port address matrix In FICON management style, an active port address matrix is the port address matrix that is currently active or operational on an attached director or switch.

active zone set A single zone set that is active in a multiswitch fabric and is created when a specific zone set is enabled. This zone set is compiled by checking for undefined zones or aliases. *See also* zone; zone set.

address (1) To refer to a device or an item of data by its address *(A, I)*. (2) The location in a computer where data is stored. (3) In data communication, the unique code assigned to each device or workstation connected to a network. (4) The identifier of a location, source, or destination *(D)*.

address name *Synonym for* port name.

address resolution protocol ARP. The protocol by which a host computer maintains a cache of address translations, allowing the physical address of the computer to be derived from the Internet address *(D)*.

alarm (1) A notification of an abnormal condition within a system that provides an indication of the location or nature of the abnormality to either a local or remote alarm indicator. (2) A simple network management protocol (SNMP) message notifying an operator of a network or device problem.

AL_PA *See* arbitrated loop physical address.

American National Standard Code for Information Interchange ASCII. A standard character set consisting of 7-bit coded characters (8-bit including parity check) used for information exchange between systems and equipment *(D)*.

American National Standards Institute ANSI. A national organization consisting of producers, consumers, and general interest groups that establishes procedures by which accredited organizations create and maintain industry standards in the United States *(A)*.

ANSI *See* American National Standards Institute.

API *See* application program interface.

application (1) The use to which a data processing system is put, for example, a payroll application, an airline reservation application, or a network application. (2) A collection of software components used to perform specific types of work on a computer *(D)*.

application client The source object of the small computer system interface (SCSI) commands and destination for the command responses.

application program (1) A program that is specific to the solution of an application problem. Synonymous with application software. (2) A program written for or by a user that applies to the user's work, such as a program that does inventory control or payroll. (3) A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities *(I)*.

application program interface API. A set of programming functions and routines that provides access between protocol layers, such as between an application and network services.

arbitrated loop One of the three connection topologies offered by Fibre Channel protocol. Up to 126 node ports and one fabric port can communicate

without the need for a separate switched fabric. *See also* point-to-point.

arbitrated loop physical address AL_PA. A 1-byte value used in the arbitrated loop topology that identifies loop ports (L_Ports). This value then becomes the last byte of the address identified for each public L_Port on the loop.

arbitration Process of selecting one device from a collection of devices that request service simultaneously.

archive (1) To copy files to a long-term storage medium for backup. (2) Removing data, usually old or inactive files, from a system and permanently storing the data on removable media to reclaim system hard disk space.

ARP *See* address resolution protocol.

ASCII *See* American National Standard Code for Information Interchange.

attribute In FICON management style, the connection status of the address on a configuration matrix: allowed, blocked, or prohibited.

availability The accessibility of a computer system or network resource.

B

b *See* bit.

B *See* byte.

backup To copy files to a second medium (disk or tape) as a precaution in case the first medium fails.

backup diskette A diskette that contains duplicate information from an original diskette. The backup diskette is used in case information on the original diskette is unintentionally changed or destroyed *(D)*.

backup field-replaceable unit Backup FRU. When an active FRU fails, an identical backup FRU takes over operation automatically (failover) to maintain director or switch and Fibre Channel link operation. *See also* active field-replaceable unit.

backup FRU *See* backup field-replaceable unit.

BB_Credit *See* buffer-to-buffer credit.

beaconing Use of light-emitting diodes (LEDs) on ports, port cards, field-replaceable units (FRUs), and directors to aid in the fault-isolation process. When enabled, active beaconing will cause LEDs to flash in order for the user to locate field-replaceable units (FRU's), switches, or directors in cabinets or computer rooms.

bit Abbreviated as b. (1) Binary digit, the smallest unit of data in computing, with a value of zero or one *(D)*. (2) A bit is the basic data unit of all digital computers. It is usually part of a data byte or data word; however, a single bit can be used to control or read logic ON/OFF functions. (3) A bit is a single digit in a binary number. Bits are the basic unit of information capacity on a computer storage device. Eight bits equals one byte.

blocked connection In FICON management style, in a director or switch, the attribute that, when set, removes the communication capability of a specific port. A blocked address is disabled so that no other address can be connected to it. A blocked attribute supersedes a dedicated or prohibited attribute on the same address. *Contrast with* unblocked connection. *See* connectivity attribute. *See also* dynamic connection; dynamic connectivity.

blocked port In a director or switch, the attribute that when set, removes the communication capability of a specific port. A blocked port continuously transmits the offline sequence.

boot (1) To start or restart a computer. (2) Loading the operating system.

bps Bits per second.

Bps Bytes per second.

buffer Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. *See* buffer-to-buffer credit.

buffer-to-buffer credit BB_Credit. (1) The maximum number of receive buffers allocated to a transmitting node port (N_Port) or fabric port (F_Port). Credit represents the maximum number of outstanding frames that can be transmitted by that N_Port or F_Port without causing a buffer overrun condition at the receiver. (2) The maximum number of

frames a port can transmit without receiving a receive ready signal from the receiving device. BB_Credit can be adjustable to provide different levels of compensation.

bus The path that carries data between the computer (microprocessor) and peripheral devices. An IDE interface cable and a small computer system interface (SCSI) cable are both examples.

bypassed port If a port is bypassed, all serial channel signals route past the port. A device attached to the port cannot communicate with other devices in the loop.

byte Abbreviated as B. A byte generally equals eight bits, although a byte can equal from four to ten bits. A byte can also be called an octet.

C

cascade Linking two or more Fibre Channel switches to form a larger switch or fabric. The switched link through fiber cables attached between one or more expansion ports (E_Ports). *See also* expansion port.

central processing unit CPU. The heart of the computer, this is the component that actually executes instructions.

central processor complex CPC. A physical grouping of hardware that includes a main storage device, one or more central processors, timers, and channels.

channel (1) A system element that controls one channel path, and whose mode of operation depends on the type of hardware attached. Each channel controls an I/O interface between the channel control element and the attached control units *(D)*. (2) Point-to-point link that transports data from one point to the other. (3) A connection or socket on the motherboard to controller card. A motherboard may have only one or two channels (primary and secondary). If a motherboard has only one channel, it may be necessary to add a controller card to create a secondary channel.

channel-attached (1) Pertaining to direct attachment of devices by data I/O channels to a computer. (2) Pertaining to devices attached to a control unit by cables, not telecommunication lines *(D)*. *Synonymous with* local.

channel path CHP. A single interface between a central processor and one or more control units, along which signals and data are sent to perform I/O requests *(D)*.

channel path identifier CHPID. In a channel subsystem, a value assigned to each channel path of the system that uniquely identifies the path *(D)*. *See also* channel-to-channel.

channel subsystem CSS. A collection of subchannels that direct the flow of information between I/O devices and main storage, relieve the processor of communication tasks, and perform path management functions *(D)*.

channel-to-channel CTC. A channel attached to another channel (channel-to-channel) and specifies the I/O mode of operation for the channel path under the I/O configuration program (IOCP) channel path identifier (CHPID) statement 'Type' parameter *(D)*. *See also* channel path identifier.

channel wrap test A diagnostic procedure that checks S/390 host-to-director or host-to-switch connectivity by returning the output of the host as input. The test is host-initiated and transmits Fibre Channel frames to a director or switch port. A director or switch port enabled for channel wrapping echoes the frame back to the host.

CHP *See* channel path.

CHAP Challenge Handshake Authentication Protocol (CHAP) provides a type of authentication between an agent (typically a network server) and the client program. Both share a predefined *secret*, which they verify during an authentication login sequence. CHAP is used with RADIUS servers to provide access authentication and accounting.

CHPID *See* channel path identifier.

Class 2 Fibre Channel service Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two node ports (N_Ports).

Class 3 Fibre Channel service Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two node ports (N_Ports).

Class F Fibre Channel service Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multiswitch fabric.

Class of Fibre Channel service Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

client A node that requests network services from a server. Typically the node is a personal computer (PC).

client/server computing Architectural model that functionally divides that execution of a unit of work between activities initiated by an end user or program (client) and those maintaining data (servers). Originally thought to make mainframes obsolete.

cluster A group of processors interconnected by a high-speed network (typically dedicated) for increased reliability and scalability. Clusters are groupings of multiple servers in which information is shared among systems. When a server in a cluster fails, one of the other servers in the cluster assumes the responsibility of the failed server, thereby ensuring server, application, and data availability.

command (1) A character string from an external source to a system that represents a request for system action. (2) A request from a terminal to perform an operation or execute a program. (3) A value sent through an I/O interface from a channel to a control unit that specifies the operation to be performed *(D)*.

community name (SNMP) A name that represents an simple network management protocol (SNMP) community that the agent software recognizes as a valid source for SNMP requests. A product recognizes a management station as a valid recipient for trap information when the station's community names are configured.

community profile Information that specifies which management objects are available to what management domain or simple network management protocol (SNMP) community name.

community (SNMP) A relationship between an simple network management protocol (SNMP) agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

component (1) Hardware or software that is part of a functional unit. (2) A functional part of an operating system; for example, the scheduler or supervisor *(D)*.

computer A programmable machine that responds to a specific set of instructions in a well-defined manner and executes a prerecorded list of instructions (a program). Computers are both electronic and digital and are made up of both hardware (the actual machine-wires, transistors, and circuits) and software (instructions and data).

concurrent firmware upgrade Firmware is upgraded without disrupting switch operation.

configuration data The collection of data that results from configuring product and system operating parameters. For example, configuring operating parameters, simple network management protocol (SNMP) agent, zoning configurations, and port configurations through the Element Manager application, results in a collection of configuration data. Configuration data includes: identification data, port configuration data, operating parameters, simple network management protocol (SNMP) configuration, and zoning configuration. A configuration backup file is required to restore configuration data if the control processor (CTP) card in a nonredundant ED-5000 Director is removed and replaced.

connectionless Nondedicated link. Typically used to describe a link between nodes which allows the switch to forward Class 2 or Class 3 frames as resources (ports) allow. Contrast this with the dedicated bandwidth that is required in a Class 1 Fibre Channel Service (FC-1) point-to-point link.

connectivity The ability of devices to link together.

connectivity attribute In FICON management style, the characteristic that determines port address status for the director or switch. *See* blocked connection; connectivity control; dynamic connection; dynamic connectivity; unblocked connection.

connectivity control In FICON management style, in a director or switch, the method used to change port address connectivity attributes and determine the communication capability of the link attached to the port *(D)*. *See also* active port address matrix; connectivity attribute.

console *See* personal computer; server.

control processor card CTP card. Circuit card that contains the director or switch microprocessor. The CTP card also initializes hardware components of the system after power-on. The card may contain an RJ-45 twisted pair connector.

credit *See* buffer-to-buffer credit.

CTP card *See* control processor card.

customer support *Synonym for* technical support.

D

data center A collection of servers and data storage devices, usually in one location, administered by an information technology/information services (IT/IS) manager.

default Pertaining to an attribute, value, or option that is assumed by a system when none is explicitly specified *(D, I)*.

default zone A zone that contains all attached devices that are not members of a separate active zone.

destination A point or location, such as a processor, director or switch, or server, to which data is transmitted *(D)*.

destination address D_ID. An address identifier that indicates the targeted destination of a data frame.

device (1) Mechanical, electrical, or electronic hardware with a specific purpose *(D)*. *See also* managed product.

(2) *See* node.

device number In a channel subsystem, four hexadecimal digits that uniquely identify an I/O device *(D)*.

diagnostics (1) The process of investigating the cause or nature of a problem in a product or system. (2) Procedures or tests used by computer users and service personnel to diagnose hardware or software problems *(D)*.

dialog box A pop-up window in the user interface with informational messages or fields to be modified or completed with desired options.

D_ID *See* destination address.

director An intelligent, highly-available, Fibre Channel switch providing any-to-any port connectivity between nodes (end devices) on a switched fabric. The director sends data transmissions (data frames)

between nodes in accordance with the address information present in the frame headers of those transmissions.

DNS name Domain name system or domain name service. Host or node name for a device or managed product that is translated to an Internet protocol (IP) address through a domain name server.

domain A Fibre Channel term describing the most significant byte in the node port (N_Port) identifier for the Fibre Channel device. It is not used in the Fibre Channel small computer system interface (FC-SCSI) hardware path ID. It is required to be the same for all SCSI targets logically connected to a Fibre Channel adapter.

domain ID Domain identifier. A number that uniquely identifies a switch in a multiswitch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch. The preferred domain ID is the domain ID value that a switch requests from the principal switch. If the value has not been allocated to another switch in the fabric, it will be granted by the principal switch and will become the requesting switch's active domain ID. The active domain ID is the domain ID that has been assigned by the principal switch and that a switch is currently using.

domain name server In TCP/IP, a server program that supplies name-to-address translation by mapping domain name to internet addresses. *(D)*

DRAM *See* dynamic random access memory.

drop-down menu A menu that appears when a heading in a navigation bar is clicked on with the mouse. The objects that appear in the drop-down menus are organize by their headings in the navigation bar.

dump The file that is created when the director detects a software fault. It contains various data fields that, when extracted, assist in the debugging of software.

dynamic connection A connection between two ports, established or removed by the directors and that, when active, appears as one continuous link. *See* connectivity attribute. *See also* blocked connection; dynamic connectivity; unblocked connection.

dynamic connectivity The capability that allows connections to be established and removed at any time.

dynamic random access memory

DRAM. Random access memory that resides in a cell comprised of a capacitor and transistor. DRAM data deteriorates (that is, is dynamic) unless the capacitor is periodically recharged by the controlling microprocessor. DRAM is slow, but relatively inexpensive *(D)*. *Contrast with* static random access memory.

E

E_D_TOV

See error-detect time-out value.

EFCM Basic interface

The interface provides a graphical user interface (GUI) similar to the Element Manager application, and supports director or switch configuration, statistics monitoring, and basic operations. With director or switch firmware installed, administrators or operators with a browser-capable personal computer (PC) and an Internet connection can monitor and manage the director or switch through an embedded web server interface.

EFCM Basic interface timeout

If the embedded web server interface is running but no user activity occurs, (such as viewing different pages, refreshing, or reconfiguring information), the application times out after 30 minutes. The user must log in again. A login dialog box displays if the user attempts to access any pages after the timeout has occurred.

EFCM Basic interface window

The window for the embedded web server interface. The window is divided into two separate panels: the navigation panel on the left, and the main panel on the right.

EIA

See Electronic Industries Association.

Electronic Industries Association

EIA. The governing body that publishes recommended standards for physical devices and associated interfaces. For example, RS-232 is the EIA standard that defines computer serial port connectivity *(D)*. *See also* Telecommunications Industry Association.

electronic mail

E-mail. Any communications service that permits the electronic transmission and storage of messages and attached or enclosed files.

Element Manager application

Application that implements the management user interface for a director or switch. (1) In your SAN management application application, the software component that provides a graphical user interface for managing and monitoring switch products. When a

product instance is opened from your SAN management application, the corresponding Element Manager application is invoked.

e-mail *See* electronic mail.

enhanced availability feature EAF. A backup field-replaceable unit (backup FRU) that is ordered and installed to provide redundancy and reduce disruption in case of failure.

enterprise The entire storage system. The series of computers employed largely in high-volume and multi-user environments such as servers or networking applications; may include single-user workstations required in demanding design, engineering and audio/visual applications.

Enterprise Systems Architecture ESA™. A computer architecture introduced by IBM in 1988 as ESA/370. The architecture added access registers to improve virtual memory management and increase storage from 2 gigabyte to 6 terabytes. The architecture was enhanced with the introduction of ESA/390 in 1990 *(D)*.

Enterprise Systems Connection ESCON™. An IBM architecture, technology, and set of products and services introduced in 1990 that provides a dynamically connected environment using fiber-optic cables as the data transmission medium *(D)*.

Enterprise Systems Connection Director ESCON™ Director. A device that provides connectivity capability and control for attaching any two links to each other through the ESCON channel. Specifically, any of the hardware devices provided for interconnecting IBM-compatible mainframe equipment through the proprietary ESCON channel connection. IBM's model numbers for ESCON directors include the 9031 and 9033.

E_Port *See* expansion port.

erase To remove electrically or magnetically stored data, leaving the space where the data was stored unoccupied *(D)*.

error-detect time-out value E_D_TOV. The time the switch waits for an expected response before declaring an error condition.

error message Indication that an error has been detected *(D)*. *See also* information message; warning message.

ESA™ *See* Enterprise Systems Architecture.

ESCON™ *See* Enterprise Systems Connection.

Ethernet A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard, which specifies the physical and software layers.

Ethernet hub A device used to connect the Management Server and the directors it manages.

event code A three-digit number that specifies the exact event that occurred. This code provides information on system failures, such as hardware failures, failure locations, or general information on normal system events.

exchange A term that refers to one of the Fibre Channel protocol "building blocks," composed of one or more nonconcurrent sequences.

expansion port E_Port. Physical interface on a Fibre Channel switch within a fabric, that attaches to an E_Port on another Fibre Channel switch through an interswitch link (ISL) to form a multiswitch fabric. *See also* fabric loop port; fabric port; generic port; hub port; node loop port; node port; segmented expansion port.

extended distance feature XDF. A means to extend the propagation distance of a fiber-optic signal.

F

fabric Entity that interconnects node ports (N_Ports) and is capable of routing (switching) Fibre Channel frames, using the destination ID information in the Fibre Channel frame header accompanying the frames. A switch is the smallest entity that can function as a complete switched fabric topology.

fabric address notification FAN. A message that informs all NL_Ports of the address of the FL_Port. Allows LIP processing to not be disruptive to FC traffic on devices that support FAN. *See* loop initialization primitive.

fabric binding A feature that enables a switch or director to communicate only with fabrics that are included in the Fabric Binding Member list (FBML). Fabric Binding is available only if the SANtegrity Binding feature is installed.

Fabric Binding Member List A list of fabric members used in fabric binding. *See* active FBML and pending FBML.

fabric element Any active director, switch, or node in a switched fabric.

fabric loop port FL_Port. A fabric port (F_Port) that contains arbitrated loop (AL) functions associated with the Fibre Channel arbitrated loop (FC-AL) topology. The access point of the fabric for physically connecting an arbitrated loop of node loop ports (NL_Ports). *See also* expansion port; fabric port; generic port; hub port; node loop port; node port; segmented expansion port.

fabric mode *See* interoperability mode.

fabric port F_Port. Physical interface within the fabric that connects to a node port (N_Port) through a point-to-point full duplex connection. *See also* expansion port; fabric loop port; generic port; hub port; node loop port; node port; segmented expansion port.

fabric services The services that implement the various Fibre Channel protocol services that are described in the standards. These services include the fabric controller (login server), name server, and server platform.

fabric switches A device which allows the communication between multiple devices using Fibre Channel protocols. A fabric switch enables the sharing bandwidth and end-nodes using basic multiplexing techniques.

failover Automatic and nondisruptive transition of functions from an active field-replaceable unit (FRU) that has failed to a backup FRU.

FAN *See* fabric address notification.

FBML *See* Fabric Binding Member List.

FC *See* Fibre Channel.

FCA *See* Fibre Channel Association.

FC-AL *See* Fibre Channel arbitrated loop.

FC adapter Fibre Channel adapter. *See* host bus adapter.

FCC Federal Communications Commission.

FCIA *See* Fibre Channel Industry Association.

FC IP *See* Fibre Channel IP address.

feature key A unique key to enable additional product features. This key is entered into the Configure Feature Key dialog box in the Element Manager application to activate optional hardware and software features. Upon purchasing a new feature, McDATA will provide the feature key to the customer.

fiber The fiber-optic cable made from thin strands of glass through which data in the form of light pulses is transmitted. It is used for high-speed transmissions over medium (200 m) to long (10 km) distances.

fiber optics The branch of optical technology concerned with the transmission of radiant power through fibers of transparent materials such as glass, fused silica, or plastic *(E)*. Telecommunication applications of fiber optics use optical fibers. A single fiber or a nonspatially aligned fiber bundle is used for each information channel. Such fibers are often called optical fibers to differentiate them from fibers that are used in noncommunication applications *(D)*.

fibre A generic Fibre Channel term used to cover all transmission media types specified in the Fibre Channel Physical Layer (FC-PH) standard such as optical fiber, copper twisted pair, and copper coaxial cable.

Fibre Channel FC. Integrated set of standards recognized by American National Standards Institute (ANSI) which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

Fibre Channel adapter FC adapter. *See* host bus adapter.

Fibre Channel address A 3-byte node port (N_Port) identifier which is unique within the address domain of a fabric. Each port may choose its own identifier, or the identifier may be assigned automatically during fabric login.

Fibre Channel arbitrated loop — FC-AL. A high-speed (100 Mbps) connection which is a true loop technology where ports use arbitration to establish a point-to-point circuit. Data can be transferred in both directions simultaneously, achieving a nominal transfer rate between two devices of 200 Mbps.

Fibre Channel Association — FCA. The FCA is a non-profit corporation consisting of over 150 members throughout the world. Its mission is to nurture and help develop the broadest market for Fibre Channel products through market development, education, standards monitoring, and fostering interoperability among members' products.

Fibre Channel fabric element — FCFE. Any device linked to a fabric.

Fibre Channel Industry Association — FCIA. A corporation consisting of over 100 computer industry-related companies. Its goal is to provide marketing support, exhibits, and tradeshows for its member companies. The FCIA complements activities of the various standards committees.

Fibre Channel IP address — FC IP. The default FC IP on a new switch is a temporary number divided by the switch's world-wide name (WWN). The system administrator needs to enter a valid IP address.

Fibre Channel standard — American National Standards Institute (ANSI) standard that provides a common, efficient data transport system that supports multiple protocols. The architecture integrates both channel and network technologies, and provides active, intelligent interconnection among devices. All data transmission is isolated from the control protocol, allowing use of point-to-point, arbitrated loop, or switched fabric topologies to meet the needs of an application.

Fibre Connection — FICON. An IBM set of products and services introduced in 1999 that is based on the Fibre Channel Standard. FICON technology uses fiber-optic cables as the data transmission medium, and significantly improves I/O performance (including one Gbps bi-directional data transfer). FICON is designed to coexist with ESCON™ channels, and FICON-to-ESCON control unit connections are supported.

fibre port module — FPM. A 1 gigabit-per-second module that contains four generic ports (G_Ports).

FICON — *See* Fibre Connection.

FICON Management Server An optional feature that can be enabled on the director or switch or switch through the Element Manager application. When enabled, host control and management of the director or switch or switch is provided through an S/390 Parallel Enterprise or 2/Series Server attached to a director or switch or switch port.

field-replaceable unit FRU. Assembly removed and replaced in its entirety when any one of its components fails *(D)*. *See* active field-replaceable unit.

file server A computer that stores data centrally for network users and manages access to that data.

firmware Embedded program code that resides and runs on, for example, directors, switches, and hubs.

FLASH memory Reusable nonvolatile memory that is organized as segments for writing, and as bytes or words for reading. FLASH memory is faster than read-only memory, but slower than random access memory *(D)*.

FL_Port *See* fabric loop port.

FPM *See* fibre port module.

F_Port *See* fabric port.

frame A variable-length packet of data that is transmitted in frame relay technology.

FRU *See* field-replaceable unit.

G

gateway address (1) In transmission control protocol/Internet protocol (TCP/IP), a device that connects two systems that use the same or different protocols. (2) In TCP/IP, the address of a router to which a device sends frames destined for addresses not on the same physical network (for example, not on the same Ethernet) as the sender. The hexadecimal format for the gateway address is XXX.XXX.XXX.XXX.

Gb *See* gigabit.

GB *See* gigabyte.

Gbps Acronym for gigabits per second.

generic port G_Port. Physical interface on a director or switch that can function either as a fabric port (F_Port) or an expansion port (E_Port), depending on the port type to which it connects. *See also* expansion port; fabric loop port; fabric port; hub port; node loop port; node port; segmented expansion port.

generic port module card GPM card. A port card that implements four generic ports (G_Ports) and provides the physical connection point for links to Fibre Channel devices.

GHz *See* gigahertz.

gigabit Gb. A unit of measure for data storage, equal to approximately 134,217,728 bytes. Approximately one eighth of a gigabyte.

gigabyte GB. A unit of measure for data storage, equal to 1,073,741,824 bytes. Generally approximated as one billion bytes *(D)*.

gigahertz GHz. One billion cycles per second (Hertz) *(D)*.

GPM card *See* generic port module card.

G_Port *See* generic port.

graphical user interface GUI. A visually oriented interface where the user interacts with representations of real-world objects displayed on the computer screen. Interactions with such objects produce actions that are intuitive to the user *(D)*.

GUI *See* graphical user interface.

H

hardware Physical equipment (director, switch, or personal computer) as opposed to computer programs or software.

HBA *See* host bus adapter.

Hertz Hz. A unit of frequency equal to one cycle per second.

heterogeneous fabric A fabric containing open-fabric-compliant products from various vendors. *Contrast with* homogeneous fabric.

hexadecimal A numbering system with base of sixteen; valid numbers use the digits 0 through 9 and characters A through F, where A represents 10 and F represents 15 *(D)*.

high availability A performance feature characterized by hardware component redundancy and concurrent maintenance. High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

homogeneous fabric A fabric consisting of only one vendor's products. *Contrast with* heterogeneous fabric.

hop (1) Data transfer from one node to another node. (2) Describes the number of switches that handle a data frame from its origination point through it's destination point.

hop count The number of hops a unit of information traverses in a fabric.

host The computer that other computers and peripherals connect to.

host bus adapter HBA. Logic card that provides a link between the server and storage subsystem, and that integrates the operating systems and I/O protocols to ensure interoperability.

hot spare *See* field-replaceable unit.

H_Port *See* hub port.

HTTP *See* hypertext transport protocol.

hub (1) In Fibre Channel protocol, a device that connects nodes into a logical loop by using a physical star topology. (2) In Ethernet, a device used to connect the Management Server and the directors it manages.

hub port H_Port. In arbitrated loop devices, a port that uses arbitrated loop protocols. The physical interface that attaches to a loop device, either an end device or another loop interconnect device (hub).

hyperlink A predefined link for jumping from one location to another, within the same computer or network site or even to a location at a

completely different physical location. Commonly used on the world wide web for navigation, reference, and depth where published text will not suffice.

hypertext transport protocol HTTP. A simple protocol that allows world wide web pages to be transferred quickly between web browsers and servers.

Hz *See* Hertz.

I

ID *See* identifier.

identifier ID. (1) One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element *(D, T)*. (2) A sequence of bits or characters that identifies a program, device, or system to another program, device, or system. *See also* port name.

IEEE *See* Institute of Electrical and Electronics Engineers.

IML *See* initial machine load.

inband management Management of the director or switch through Fibre Channel. An interface connection to a port card. *Contrast with* out-of-band management.

industry standard architecture ISA. Bus architecture designed for personal computers (PCs) that use an Intel 80386, 80486, or Pentium microprocessor. ISA buses are 32 bits wide and support multiprocessing.

Infiniband The name applied to the merged specifications for Next Generation Input Output (NCGIO) from Intel and System IO from Compaq, HP, and IBM. Infiniband is a serial interconnect technology with a wire/fiber data speed of 2.5 GB. The basic Infiniband is a full-duplex dual wire/fiber.

information message Message notifying a user that a function is performing normally or has completed normally. *See also* error message; warning message.

information services IS. IS is the name of the department responsible for computers, networking, and data management. *See also* information technology.

information technology — IT. The broad subject concerned with all aspects of managing and processing information, especially within a large organization or company. Because computers are central to information management, computer departments within companies and universities are often called IT departments. *See also* information services.

initial machine load — IML. Hardware reset for all installed control processor (CTP) cards on the director or switch. This reset does not affect other hardware. It is initiated by pushing the IML button on a director's or switch's operating panel.

initial program load — IPL. The process of initializing the device and causing the operating system to start. An IPL may be initiated through a menu option or a hardware button.

initial program load configuration — IPL configuration. In S/390 mode, information stored in a director or switch's nonvolatile memory that contains default configurations. The director or switch loads the file for operation when powered on.

input/output — I/O. (1) Pertaining to a device whose parts can perform an input process and an output process at the same time *(I)*. (2) Pertaining to a functional unit or channel involved in an input process, output process, or both, concurrently or not, and to the data involved in such a process. (3) Pertaining to input, output, or both *(D)*. (4) An operation or device that allows input and output.

Institute of Electrical and Electronics Engineers — IEEE. An organization of engineers and technical professionals that promotes the development and application of electronic technology and allied sciences.

integrated product — Hardware product that is mounted in a cabinet. For example, any director or switch shipped within a cabinet is an integrated product.

interface — (1) A shared boundary between two functional units, defined by functional, signal, or other characteristics. The concept includes the specification of the connection of two devices having different functions *(T)*. (2) Hardware, software, or both, that link systems, programs, or devices *(D)*.

interface controller — The chip or circuit that translates computer data and commands into a form suitable for use by the hard drive and controls the transfer of data between the buffer and the host.

Internet protocol IP. Network layer for the transmission control protocol/Internet protocol (TCP/IP) protocol used on Ethernet networks. IP provides packet routing, fragmentation, and reassembly through the data link layer *(D)*.

Internet protocol address IP address. Unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a device on a network.

interoperability Ability to communicate, execute programs, or transfer data between various functional units over a network.

interoperability mode Interop mode. A management style set through management software that allows products to operate in homogeneous or heterogeneous fabrics.

interop mode *See* interoperability mode.

interswitch link ISL. Physical expansion port (E_Port) connection between two directors in a fabric.

interswitch link hop ISL hop. *See* hop.

intranet A private version of the Internet that provides a cost-effective way to publicize critical information and that provides an interactive communication path for heterogeneous systems. Internal to a specific organizational structure and secured from or disconnected from the global Internet.

I/O *See* input/output.

IP *See* Internet protocol.

IP address *See* Internet protocol address.

IPL *See* initial program load.

IPL configuration *See* initial program load configuration.

IS *See* information services.

ISL *See* interswitch link.

ISL hop Interswitch link hop. *See* hop.

isolated E_Port Isolated expansion port. *See* segmented expansion port.

isolated expansion port Isolated E_Port. *See* segmented expansion port.

IT *See* information technology.

K

Kb *See* kilobit.

KB *See* kilobyte.

kilobit Kb. A unit of measure for data storage, equaling 1,024 bits, or two to the tenth power. Kilobits are generally approximated as being one thousand bits.

kilobyte KB. A unit of measure for data storage, equaling 1,024 bytes, or two to the tenth power. Kilobytes are generally approximated as being one thousand bytes.

L

LAN *See* local area network.

laser Laser is an acronym for light amplification by stimulated emission of radiation. A device that produces a very powerful narrow beam of coherent light of a single wavelength by simulating the emissions of photons from atoms, molecules, or ions.

latency Amount of time elapsed between receipt of a data transmission at a switch's incoming fabric port (F_Port) from the originating node port (N_Port) to retransmission of that data at the switch's outgoing F_Port to the destination N_Port. The amount of time it takes for data transmission to pass through a switching device.

LED *See* light-emitting diode.

light-emitting diode LED. A semiconductor chip that emits visible or infrared light when electricity passes through it. LEDs are used on switch or director

field-replaceable units (FRUs) and the front bezel to provide visual indications of hardware status or malfunctions.

LIN *See* link incident.

link Physical connection between two devices on a switched fabric. A link consists of two conductors, one used for sending and the other for receiving, thereby providing a duplex communication path.

link incident LIN. Interruption to link due to loss of light or other causes. *See also* link incident alerts.

link incident alerts A user notification, such as a graphic symbol in the Element Manager application *Hardware View* that indicates that a link incident has occurred. *See also* link incident.

LIP *See* loop initialization primitive.

load balancing Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on McDATA directors and switches takes place automatically.

local *Synonym for* channel-attached.

local area network LAN. A computer network in a localized geographical area (for example, a building or campus), whose communications technology provides a high-bandwidth medium to which many nodes are connected *(D)*. *See also* storage area network; wide area network.

logical unit number LUN. In Fibre Channel addressing, a logical unit number is a number assigned to a storage device which, in combination with the storage device's node port's world-wide name, represents a unique identifier for a logical device on a storage area network. Peripherals use LUNs to represent addresses. A small computer system interface (SCSI) device's address can have up to eight LUNs.

login server Entity within the Fibre Channel fabric that receives and responds to login requests.

loop A loop is a configuration of devices connected to the fabric via a fabric loop port (FL_Port) interface card.

loop address In Fibre Channel protocol, a term indicating the unique ID of a node in Fibre Channel loop topology, sometimes referred to as a loop ID.

loopback plug In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input. *Contrast with* protective plug. *Synonymous with* wrap plug.

loopback test Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

loop initialization primitive LIP. In an arbitrated loop device, a process by which devices connected to hub ports (H_Ports) on the arbitrated loop device notify other devices and the switch of the presence in the loop by sending LIP sequences and subsequent frames through the loop. This process allows linked arbitrated loop devices to perform fabric loop port (FL_Port) arbitration as they link through hub ports.

loop master In an arbitrated loop device, a reference to the loop master world-wide name (WWN) field in the *Loop View*, the loop master is the arbitrated loop device that is responsible for allocating arbitrated loop physical addresses (AL-PAs) on the loop. An arbitrated loop device becomes the loop master through arbitration when there are multiple arbitrated loop devices on the loop. The arbitrated loop device with the lowest WWN becomes the loop master.

loop port L_Port. *Synonym for* hub port.

loop switches Loop switches support node loop port (NL_Port) Fibre Channel protocols. Switches sold as loop support but upgradeable to fabric switches recounted as loop switches.

L_Port Loop port. *Synonym for* hub port.

LUN *See* logical unit number.

M

maintenance port Connector on the director or switch where a PC running an American National Standard Code for Information Interchange (ASCII) terminal emulator can be attached or dial-up connection made for specialized maintenance support.

managed product Hardware product that can be managed with the Element Manager application. Directors and switches are managed products. *See also* device.

management information base MIB. Related set of software objects (variables) containing information about a managed device and accessed via simple network management protocol (SNMP) from a network management station.

management session A session that exists when a user logs on to your SAN management application. The SAN management application can support multiple concurrent management sessions. The user must specify the network address of your SAN management application's server at logon time.

matrix *See* active port address matrix.

Mb Megabit.

MB *See* megabyte.

Mbps Megabits per second.

MBps Megabytes per second.

megabyte MB. A unit of measure for data storage, equal to 1,048,576 bytes. Generally approximated as one million bytes.

memory A device or storage system capable of storing and retrieving data.

menu A list of items displayed on a monitor from which a user can make a selection.

menu bar The menu bar is located across the top of a monitor window. Pull-down menus are displayed by clicking on the menu bar option with the mouse, or by pressing **Alt** with the underlined letter of the name for the menu bar option *(D)*.

message path controller card MPC card. In the ED-5000 Director, a card that provides the mechanism for messages to be sent and received between ports on the director. The card also provides a system clock source, and central control and distribution of clocks for MPC, G_Port module (GPM), and central memory module (CMM) cards.

MIB *See* management information base.

modem Modem is an abbreviation for modulator/demodulator. A communication device that converts digital computer data to signals and signals to computer data. These signals can be received or transmitted by the modem via a phone line or other method of telecommunication.

MPC card *See* message path controller card.

ms Millisecond.

multimedia A simultaneous presentation of data in more than one form, such as by means of both visual and audio.

multiswitch fabric Fibre Channel fabric created by linking more than one director or fabric switching device within a fabric.

N

name server (1) In TCP/IP, *see* domain name server. (2) In Fibre Channel protocol, a server that allows node ports (N_Ports) to register information about themselves. This information allows N_Ports to discover and learn about each other by sending queries to the name server.

name server zoning Node port (N_Port) access management that allows N_Ports to communicate if and only if they belong to a common name server zone.

navigation panel The left side of the embedded web server interface window. Click on words in this panel to display menu options.

network An arrangement of hardware, software, nodes, and connecting branches that comprises a data communication system. The International Organization for Standardization (ISO) seven-layer specification partitions a computer network into independent modules from the lowest (physical) layer to the highest (application) layer *(D)*.

network address Name or address that identifies a device on a transmission control protocol/Internet protocol (TCP/IP) network. The network address can be either an IP address in dotted-decimal notation (composed of four three-digit octets in the format xxx.xxx.xxx.xxx) or a domain name (as administered on a customer network).

network-attached storage NAS. Storage connected directly to the network, through a processor and its own operating system. Lacks the processor power to run centralized, shared applications.

network management The broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including security, performance, and reliability.

nickname Alternate name assigned to a world-wide name for a node, director or switch in the fabric.

NL_Port *See* node loop port.

node In Fibre Channel protocol, an end device (server or storage device) that is or can be connected to a switched fabric. *See also* device.

node loop port NL_Port. A physical interface within an end device (node) that participates in a loop containing one or more fabric loop ports (FL_Ports) or other NL_Ports. *See also* expansion port; fabric loop port; fabric port; generic port; hub port; node port; segmented expansion port.

node port N_Port. Physical interface within an end device that can connect to an fabric port (F_Port) on a switched fabric or directly to another N_Port (in point-to-point communications). *See also* expansion port; fabric loop port; fabric port; generic port; hub port; node loop port; segmented expansion port.

node port identifier N_Port ID. In Fibre Channel protocol, a unique address identifier by which an N_Port is uniquely known. It consists of a domain (most significant byte), an area, and a port, each 1 byte long. The N_Port ID is used in the source identifier (S_ID) and destination identifier (D_ID) fields of a Fibre Channel frame.

nonvolatile random access memory NV-RAM. RAM that retains its content when the device power is turned off.

N_Port *See* node port.

N_Port ID *See* node port identifier.

NV-RAM *See* nonvolatile random access memory.

O

OEM *See* original equipment manufacturer.

offline Referring to data stored on a medium, such as tape or even paper, that is not available immediately to the user.

offline diagnostics Diagnostics that only operate in stand alone mode. User operations cannot take place with offline diagnostics running.

offline sequence OLS. (1) Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so. (2) Sequence sent by the transmitting port to indicate that it is offline.

offline state When the switch or director is in the offline state, all the installed ports are offline. The ports transmit an offline sequence (OLS) and they cannot accept a login got connection from an attached device. *Contrast with* online state.

OLS *See* offline sequence.

online Referring to data stored on the system so it is available immediately to the user.

online diagnostics Diagnostics that can be run by the customer engineer while the operational software is running. These diagnostics do not impact user operations.

online state When the switch or director is in the online state, all of the unblocked ports are allowed to log into the fabric and begin communicating. Devices can connect to the switch or director if the port is not blocked and can communicate with another attached device if both devices are in the same zone, or if the default zone is enabled. *Contrast with* offline state.

Open Systems Architecture OSI. A model that represents a network as a hierarchical structure of functional layers. Each layer provides a set of functions that can be accessed and used by the layer above. Layers are independent, in that implementation of a layer can be changed without affecting other layers *(D)*.

open systems management server OSMS. An optional feature, when enabled, host control and management of the director or switch are provided through an Open

System Interconnection (OSI) device attached to a director or switch port.

OpenTrunking OpenTrunking is a licensed optional feature that enables load balancing of traffic flows. OpenTrunking monitors the average speed of data traffic through a flow. In the event of traffic congestion, or if traffic on an ISL is disproportionate, a traffic flow is rerouted to a less congested ISL. See also interswitch link.

operating system OS. Software that controls execution of applications and provides services such as resource allocation, scheduling, I/O control, and data management. Most operating systems are predominantly software, but partial hardware implementations are possible *(D, T)*.

Operating System/390 OS/390™. An integrated, open-enterprise server operating system developed by IBM that incorporates a leading-edge and open communications server, distributed data and file services, parallel Sysplex™ support, object-oriented programming, distributed computing environment, and open application interfaces *(D)*.

original equipment manufacturer OEM. A company that has a special relationship with computer producers. OEMs buy components and customize them for a particular application. They sell the customized computer under their own name. OEMs may not actually be the original manufacturers. They are usually the customizers and marketers.

OS *See* operating system.

OS/390™ *See* Operating System/390.

OSI *See* Open Systems Architecture.

OSMS See open systems management server.

out-of-band management Transmission of management information, using frequencies or channels other than those routinely used for information transfer.

P

packet In Fibre Channel protocol, Logical unit of information (usually in the form of a data frame) transmitted on a network. It contains a header (with all relevant addressing and timing information), the actual

data, and a trailer (which contains the error checking function, usually in the form of a cyclic redundancy check), and frequently user data.

panel A logical component of the interface window. Typically, a heading and/or frame marks the panel as an individual entity of the window. Size and shape of the panel and its data depend upon the purpose of the panel and may or may not be modified.

PC *See* personal computer.

pending FBML The pending Fabric Binding Member list. A list of fabric binding members, shown on the *Fabric Binding* tab, which is not active on the product. It is made active on the switch or director using the *Fabric Binding* tab. *Contrast with* active FBML and Fabric Binding Member List.

persistent binding A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device), using a unit number. *See also* access control.

personal computer PC. A portable computer that consists of a system unit, display, keyboard, mouse, one or more diskette drives, and internal fixed-disk storage *(D)*.

point-to-point A Fibre Channel protocol topology that provides a single, direct connection between two communication ports. The director or switch supports only point-to-point topology. *See also* arbitrated loop.

port Receptacle on a device to which a cable leading to another device can be attached. Ports provide Fibre Channel connections *(D)*.

port address name A user-defined symbolic name of 24 or fewer characters that identifies a particular port address.

port authorization Feature of the password definition function that allows an administrator to extend operator-level passwords to specific port addresses for each director or switch definition managed by a personal computer (PC). Port authorization affects only operator-level actions for active and saved matrices *(D)*.

port binding Configuring a specific switch or director port to communicate exclusively with an attached device.

port card Field-replaceable hardware component that provides the port connections for fiber cables and performs specific device-dependent logic functions.

port card map Map showing port numbers and port card slot numbers inside a hardware cabinet.

port name Name that the user assigns to a particular port through the Element Manager application. *See also* identifier. *Synonymous with* address name.

preferred domain ID Configured value that a switch will request from the Principal Switch. If the preferred value is already in use, the Principal Switch will assign a different value.

principal switch In a multiswitch fabric, the switch that allocates domain IDs to itself and to all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.

private device A loop device that cannot transmit a fabric login command (FLOGI) command to a switch or director, nor communicate with fabric-attached devices. *Contrast with* public device.

private loop A private loop is not connected to a switched fabric, and the switch's embedded expansion port (E_Port) and fabric loop port (FL_Port) are inactive. All devices attached to the loop can only communicate with each other. *Contrast with* public loop.

product name User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. A director or switch product name can also be accessed by a simple network management protocol (SNMP) manager as the system name.

prohibited port connection In a director or switch, in S/390 operating mode, an attribute that removes dynamic connectivity capability.

proprietary Privately owned and controlled. In the computer industry, proprietary is the opposite of open. A proprietary design or technique is one that is owned by a company. It also implies that the company has not divulged specifications that would allow other companies to duplicate the product. Increasingly, proprietary architectures are seen as a disadvantage. Consumers prefer open and

standardized architectures, which allow them to mix and match products from different manufacturers.

protective plug In a fiber-optic environment, a type of duplex connector (or cover) that provides physical protection *(D)*. *Contrast with* loopback plug.

protocol (1) Set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (2) In systems network architecture, the meanings of and sequencing rules for requests and responses for managing the network, transferring data, and synchronizing network component states. (3) A specification for the format and relative timing of data exchanged between communicating devices *(D, I)*.

public device A loop device that can transmit a fabric login command (FLOGI) to a switch, receive acknowledgement from the switch's login server, register with the switch's name server, and communicate with fabric-attached devices. Public devices communicate with fabric-attached devices through the switch's bridge port (B_Port) connection to a director or switch. *Contrast with* private device.

public loop A public loop is connected to a switched fabric (through the switch bridge port (B_Port)), and the switch has an active embedded fabric loop port (FL_Port) that is user transparent. All devices attached to the loop can communicate with each other, and public devices attached to the loop can communicate with fabric-attached devices. *Contrast with* private loop.

pull-down menu *See* drop-down menu.

R

RAID *See* redundant array of independent disks.

RAM *See* random access memory.

random access memory RAM. A group of computer memory locations that is numerically identified to allow high-speed access by the controlling microprocessor. A memory location is randomly accessed by referring to its numerical identifier *(D)*. *Contrast with* read-only memory. *See* also dynamic random access memory; nonvolatile random access memory; static random access memory.

R_A_TOV *See* resource allocation time-out value.

read-only memory ROM. An information storage chip with permanent memory. Stored information cannot be changed or deleted except under special circumstances *(D)*. *Contrast with* random access memory.

redundancy Performance characteristic of a system or product whose integral components are backed up by identical components to which operations will automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hours/7 days per week) computer systems and networks.

redundant array of independent disks RAID. Grouping of hard drives in a single system to provide greater performance and data integrity. RAID systems have features that ensure data stored on the drives are safe and quickly retrievable.

remote notification A process by which a system is able to inform remote users of certain classes of events that occur on the system. E-mail notification and the configuration of simple network management protocol (SNMP) trap recipients are two examples of remote notification programs that can be implemented on director-class switches.

rerouting delay An option that ensures that frames are delivered in order through the fabric to their destination.

resource allocation time-out value R_A_TOV. R_A_TOV is a value used to time-out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

ring topology A logically circular, unidirectional transmission path without defined ends, in which control is distributed or centralized *(D)*. *See also* token ring.

RS-232 The Electronic Industry Association (EIA)-recommended specification for asynchronous serial interfaces between computers and communications equipment. It specifies both the number of pins and type of connection, but does not specify the electrical signals *(D)*.

S

SAN *See* storage area network; system area network.

SANavigator SANavigator management software provides easy, centralized management of a SAN and quick access to all device configuration applications.

SANavigator Server The computer that is hosting the SANavigator application. Multiple client systems can log into the Server to utilize the application.

SBAR *See* serial crossbar assembly.

SBML *See* switch binding membership list.

scalable Refers to how well a system can adapt to increased demands. For example, a scalable network system could start with just a few nodes but easily expands to thousands of nodes. Scalability is important because it allows the user to invest in a system with confidence that a business will not outgrow it. Refers to anything whose size can be changed.

SCSI *See* small computer system interface.

segment A fabric segments when one or more switches cannot join the fabric because of various reasons. The switch or switches remain as separate fabrics.

segmented E_Port *See* segmented expansion port.

segmented expansion port Segmented E_Port. E_Port that has ceased to function as an E_Port within a multiswitch fabric due to an incompatibility between the fabrics that it joins. *See also* fabric loop port; fabric port; generic port; hub port; node loop port; node port.

serial crossbar assembly SBAR. The assembly is responsible for Fibre Channel frame transmission from any director or switch port to any other director or switch port. Connections are established without software intervention.

serial port A full-duplex channel that sends and receives data at the same time. It consists of three wires: two that move data one bit at a time in opposite directions, and a third wire that is a common signal ground wire.

server A computer that provides shared resources, such as files and printers, to the network. Used primarily to store data, providing access to shared resources. Usually contains a network operating system.

shared mode
If a director or switch is in shared mode, all devices on the loop share the 100 MB bandwidth available on the loop. In shared mode, only one end device can communicate with another device through the fabric loop port (FL_Port) on the director or switch.

simple mail transfer protocol
SMTP. A transmission control protocol/Internet protocol (TCP/IP) protocol that allows the user to create, send, and receive text messages. SMTP protocols specify how messages are passed across a link from one system to another. They do not specify how the mail application accepts, presents, or stores the mail.

simple network management protocol
SNMP. A transmission control protocol/Internet protocol (TCP/IP)-derived protocol governing network management and monitoring of network devices.

simple network management protocol community
SNMP community. Also known as SNMP community string. SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which the server or managed product running the SNMP agent belongs.

simple network management protocol community name
SNMP community name. The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent will only elicit a response if those queries are addressed with the correct SNMP community name.

simple network management protocol management station
SNMP management station. An SNMP workstation personal computer (PC) used to oversee the SNMP network.

simple network management protocol version 1
SNMP v1. The original standard for SNMP is now referred to as SNMP v1.

simple network management protocol version 2
SNMP v2. The second version of the SNMP standard. This version expands the functionality of SNMP and broadens its ability to include OSI-based, as well as TCP/IP-based, networks as specified in RFC 1441 through 1452.

small computer system interface
SCSI. An interface standard that enables computers to communicate with peripherals connected to them. Commonly used in enterprise computing and in Apple Macintosh systems. Usually pronounced as "scuzzy." The equivalent interface in most personal computers is enhanced integrated drive electronics (EIDE).

A narrow SCSI adapter supports up to eight devices, including itself. SCSI address 7 has the highest priority followed by 6, 5, 4, 3, 2, 1, 0, with 0 being the lowest priority.

SNMP *See* simple network management protocol.

SNMP community *See* simple network management protocol community.

SNMP community name *See* simple network management protocol community name.

SNMP management station *See* simple network management protocol management station.

SNMP v1 *See* simple network management protocol version 1.

SNMP v2 *See* simple network management protocol version 2.

SRAM *See* static random access memory.

SSP *See* system services processor.

state The state of the switch or director. Possible values include online, offline, testing, and faulty. See offline state; online state.

static random access memory SRAM. SRAM is microprocessor-cache random access memory. It is built internal to the microprocessor or on external chips. SRAM is fast, but relatively expensive *(D)*. *Contrast with* dynamic random access memory.

storage area network SAN. A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated. *See also* local area network; wide area network.

stored addresses In FICON management style, a method for configuring addresses.

subnet A portion of a network that shares a common address component. On transmission control protocol/Internet protocol (TCP/IP) networks, subnets are defined as all devices whose IP addresses have the same prefix. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

subnet mask A mask used by a computer to determine whether another computer with which it needs to communicate is located on a local or remote network. The network mask depends upon the class of networks to which the computer is connecting. The mask indicates which digits to look at in a longer network address and allows the router to avoid handling the entire address. Subnet masking allows routers to move the packets more quickly. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network.

switch A device that connects, filters and forwards packets between local area network (LAN) segments or storage area network (SAN) nodes or devices.

switch binding A feature that restricts the product from allowing connections with the devices that are not listed on the Switch Binding Membership List. Switch Binding is available only if the SANtegrity Binding feature is installed.

switch binding membership list SBML. If switch binding is enabled, a list of devices with which the product is allowed to make connections.

switched mode If the arbitrated loop device is in switched mode, each pair of communicating ports on the arbitrated loop device can share the 100 Mb bandwidth. In switched mode, up to three pairs of loop devices can communicate with each other simultaneously. Or, a public device on the loop can communicate with another device on the fabric while up to two pairs of loop devices can communicate simultaneously.

switchover Changing a backup field-replaceable unit (FRU) to the active state, and the active FRU to the backup state.

switch priority Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric's principal switch. Lower values indicate higher likelihood of becoming the principal switch. A value of 1 indicates the highest priority; 225 is the lowest priority. A value of 225 indicates that the switch is not capable of acting as the principal switch. The value 0 is illegal.

system name *See* product name.

system services processor SSP. In a director or switch, the central controlling processor. Controls the RS-232 maintenance port and the Ethernet port of a Fibre Channel director or switch.

T

TB *See* terabyte.

TCP *See* transmission control protocol.

TCP/IP *See* transmission control protocol/Internet protocol.

technical support Single point of contact for a customer when assistance is needed in managing or troubleshooting a product. Technical support provides assistance twenty-four hours a day, seven days a week, including holidays. The technical support number is **(800) 752-4572** or **(720) 566-3910**. *Synonymous with* customer support.

Telecommunications Industry Association TIA. A member organization of the Electronic Industries Association (EIA), TIA is the trade group representing the communications and information technology industries. *See also* Electronic Industries Association.

telnet The Internet standard protocol for remote terminal connection over a network connection.

terabyte TB. One thousand (1,000) gigabytes; one terabyte of text on paper would consume 42,500 trees. At 12 characters per inch, 1 TB of data in a straight line would encircle the earth 56 times and stretch some 1.4 million miles equalling nearly three round trips from the earth to the moon.

TIA *See* Telecommunications Industry Association.

token A sequence of bits passed from one device to another on a token ring network that signifies permission to transmit over the network. The token consists of a starting delimiter, access control field, and end delimiter. If a device has data to transmit, it appends the data to the token *(D)*.

token ring A local area network (LAN) configuration where devices attach to a network cable in a closed path or ring. A token (unique sequence of

bits) circulates on the ring to allow devices to access the LAN for data transmission *(D)*. *See also* ring topology.

token ring controller adapter card TKRG. The circuit card that provides a port to connect a director or switch to a 4/16 Mbps token ring local area network (LAN) *(D)*.

topology Logical and/or physical arrangement of stations on a network.

transceiver modules Transceiver modules come in longwave, extra longwave, or shortwave laser versions, providing a single fiber connection.

transfer rate The speed with which data can be transmitted from one device to another. Data rates are often measures in megabits (Mbps) or megabytes (MBps) per second, or gigabits per second (Gbps) or gigabytes per second (GBps).

transmission control protocol TCP. The transport layer for the transmission control protocol/Internet protocol (TCP/IP) protocol widely used on Ethernet networks and any network that conforms to U.S. Department of Defense standards for network protocol. TCP provides reliable communication and control through full-duplex connections *(D)*.

transmission control protocol/Internet protocol TCP/IP. A layered set of protocols (network and transport) that allows sharing of applications among devices on a high-speed local area network (LAN) communication environment *(D)*. *See also* transmission control protocol; Internet protocol.

trap Unsolicited notification of an event originating from a simple network management protocol (SNMP) managed device and directed to an SNMP network management station.

trap host Simple network management protocol (SNMP) management workstation that is configured to receive traps.

trap recipient In simple network management protocol (SNMP), a network management station that receives messages through SNMP for specific events that occur on the arbitrated loop device.

U

UDP *See* user datagram protocol.

UL — *See* Underwriters Laboratories.

unblocked connection — In a director or switch, the absence of the blocked attribute for a specific port. *Contrast with* blocked connection. *See* connectivity attribute. *See also* dynamic connection; dynamic connectivity.

unblocked port — Devices communicating with an unblocked port can log into the director or switch and communicate with devices attached to any other unblocked port (assuming that this is supported by the current zoning configuration).

Underwriters Laboratories — UL. A laboratory organization accredited by the Occupational Safety and Health Administration and authorized to certify products for use in the home and workplace *(D)*.

uniform resource locator — URL. A URL is the address of a document or other resource on the Internet.

uninterruptable power supply — UPS. A buffer between public utility power or another power source, and a system that requires precise, uninterrupted power *(D)*.

universal port module — UPM. A flexible 1 gigabit-per-second or 2 gigabit-per-second module that contains four generic ports (G_Ports).

UNIX — A popular multi-user, multitasking operating system originally designed to be a small, flexible system used exclusively by programmers. UNIX was one of the first operating systems to be written in a high-level programming language, namely C. This meant that it could be installed on virtually any computer for which a C compiler existed. Due to its portability, flexibility, and power, UNIX has become the leading operating system for workstations. Historically, it has been less popular in the personal computer market, but the emergence of a new version called Linux is revitalizing UNIX across all platforms.

UPM — *See* universal port module.

UPS — *See* uninterruptable power supply.

URL — *See* uniform resource locator.

user datagram protocol — UDP. A connectionless protocol that runs on top of Internet protocol (IP) networks. User datagram protocol/Internet protocol (UDP/IP) offers very few error recovery services, instead providing a direct

way to send and receive datagrams over an IP network. UDP/IP is primarily used for broadcasting messages over an entire network. *Contrast with* transmission control protocol/Internet protocol.

V

vital product data VPD. System-level data stored by field-replaceable units (FRUs) in the electrically erasable programmable read-only memory. This data includes serial numbers and identifies the manufacturer.

VPD *See* vital product data.

W

WAN *See* wide area network.

warning message A message that indicates a possible error has been detected. *See also* error message; information message.

wide area network WAN. A network capable of transmission over large geographic areas that uses transmission lines provided by a common-carrier. *See also* local area network; storage area network.

window The main window for the SAN management or Element Manager applications. Each application has a unique window that is divided into separate panels for the title, navigation control, alerts, and the main or *Product View*. The user performs all management and monitoring functions for these Fibre Channel products through the application window.

Windows A graphical user interface and windowing system introduced by Microsoft Corporation in 1985. Windows runs on top of the MS-DOS operating system *(D)*.

workstation A terminal or microcomputer usually connected to a network or mainframe at which a user can perform applications.

world wide names WWN. Eight-byte string that uniquely identifies a Fibre Channel entity (that is, a port, a node, a switch, a fabric), even on global networks.

wrap plug *Synonym for* loopback plug.

wrap test A test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input. A wrap test can transmit a specific character pattern through a system and compare the pattern received with the pattern transmitted *(D)*.

write authorization Permission for an simple network management protocol (SNMP) management station with the proper community name to modify writable management information base (MIB) variables.

WWN *See* world wide names.

X

XDF *See* extended distance feature.

Z

zone Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can see each other. Those devices that occupy different zones cannot. *See also* active zone set; zone set; zoning.

zone member Specification of a device to be included in a zone. A zone member can be identified by the port number of the director or switch to which it is attached or by its port world-wide name (WWN). In multiswitch fabrics, identification of end-devices or nodes by WWN is preferable.

zone set A collection of zones that may be activated as a unit. *See also* active zone set; zone.

zoning Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the director or switch,

may be configured into one or more zones. *See also* access control; zone.

Index

Symbols

3-12

A

activating
    beaconing 7-5
    zone sets 4-17
active domain ID 2-12
active zone set, description 4-10
address
    IP, see IP address
    resolution protocol table 3-17
alert symbols 2-2
ARP table 3-17
attached port WWN 2-8
audience for manual xv
authorization
    write 3-19
authorization traps 3-18

B

basic information
    port 3-2
BB_Credit 2-14
    configure 3-5
Beacon page 7-5
beaconing 2-8
    ports 7-5
binding 4-5
block
    port 3-3
block configuration 2-5, 2-8
blocking a port 2-8
blocking ports 2-5
browser
    logging in 1-7
browser level required 1-3

C

class of service 2-14
CLI 1-2
    enable and disable 3-19, 3-33
codes, error event 6-3
command line interface 3-19
    enable and disable 3-33
community name 3-19
configure
    BB_Credits 3-5
    date and time 3-10
    fabric parameters 3-14
    identification 3-9
    NPIV 3-7
    port fencing 3-30
    port information 3-2
    preferred path 3-28
    security 5-1
    SNMP 3-18
    switch parameters 3-11
    zoning 4-13, 4-14, 4-17
Configure menu 3-1
configuring
    product identification 3-9
contact, product 2-3, 3-10
controlling access
    fabric 4-2

server or storage device 4-5
server-level 4-5
conventions used in manual xvi
conventions, naming 4-7
COS 2-14
cost configuration, ISL FSPF 3-13
counter 2-15
CTP dump file 7-9

D

data field size, RX 2-14
date 3-10
date fields 3-10
Date Time view 3-10
deactivating
beaconing 7-5
zone sets 4-17
default
user name 1-3, 1-8, 3-17
values, factory 3-2
zone
concepts 4-9
definition
interface terms 1-10
wraps 2-15
delay, rerouting 2-12, 3-12
description
active zone set 4-10
EFCM Basic 1-1
product 2-3, 3-10
zone sets 4-9
zones 4-7
diagnostic, loopback 7-7
director speed 2-13
disable
CLI 3-19
host control 3-20
OSMS 3-20
SNMP agent 3-18
zoning 4-10
documentation
forwarding comments xvii
ordering xviii
related xvi
Domain
Fibre Channel Address 2-12
domain ID
active 2-12
insistent 2-12, 3-11, 5-24
numbers 4-8
preferred 2-12, 3-13
unique 3-13
zoning
changes and consequences 4-9
domain RSCN 2-13
enable 3-12
domain RSCNs
enterprise fabric mode 5-24
driver, HBA 4-5
dump file, retrieving 7-9

E

E/OS 1-1
E_D_TOV 2-13, 3-15
E_Port 2-7, 3-4
domain ID 3-13
E_D_TOV 3-15
enable switch binding for 5-31
R_A_TOV 3-15
segmented 2-8, 4-11, 4-12
EC level 2-4
EFC Manager 1-1
EFCM 1-1, 1-7, 10-1
scalability 10-2
EFCM Basic
benefits of 1-4
description 1-1
functionality 10-1
starting 1-7
tasks 1-2
where to start 1-6
Element Manager 1-1, 4-8
Element Manager, installing 9-3
enable
authorization traps 3-18
CLI 3-19
host control 3-20, 3-21
OSMS 3-20
SNMP agent 3-18
engineering change level 2-4
Enter Network Password dialog box 1-7
enterprise fabric mode 5-23

features and parameters enabled by 5-22
error
event codes 6-3
statistics 2-18
Error Detection Time Out Value 2-13
event codes 6-3
external loopback test 7-7

F

F_Port 2-7, 3-4
enable switch binding for 5-31
FA MIB version 3-18
fabric
address notification feature 3-3
controlling access to 4-2
creating 4-11
definition 1-5
merging 4-11
SANavigator 10-2
fabric binding
enterprise fabric mode 5-23
online state functions 5-26
fabric parameters view 3-14
factory default values 3-2
FAN 2-8
feature 3-3
status 2-8
FC-AL devices 3-3
fencing, port 3-30
Fibre Channel Arbitrated Loop devices 3-3
Fibre Channel Domain 2-12
Fibre Channel storage volume 4-5
FICON 1-2
field size, RX 2-14
firmware 1-1
level 2-4
upgrading 7-13
Flexport, installing 9-3
FMS 1-2
frames
routing of 2-12
too short, error statistics 2-18
front view 2-2
FRU
name 2-11
part number 2-11
position 2-11
serial number 2-11
status 2-11
FRU List 2-11
FSPF cost configuration 3-13
full volatility feature, installing 9-3
FX_Port 2-7, 3-4

G

G_Port 2-7, 3-4
gateway address 3-2
setting 3-17
GX_Port 2-7, 3-4

H

hardware view, alert symbol function 2-2
HBA
driver 4-5
zone member ID 4-8
help
internet access xvii
technical support xvii
hop counts 2-12
host bus adapter driver 4-5
host control 3-21
enable and disable 3-20
HTML, browser levels 1-3

I

identification page 3-9
indicator lights 2-2
insistent domain ID 2-12, 3-11
enterprise fabric mode 5-24
installing
Element Manager 9-3
Flexport 9-3
full volatility 9-3
NPIV 9-3
OpenTrunking feature 9-3
SANtegrity Authentication 9-3
SANtegrity Binding 9-3
integration of applications 10-2
interface terminology 1-10
internal loopback test 7-7
interop mode 2-13, 4-7

defining 3-15
introduction to EFCM Basic 1-1
IP 1-7
IP address 3-2, 3-17
product 1-7
setting 3-17
IPL
limit fabric RSCNs 3-12
ISL FSPF cost configuration 3-13

K

key terms 1-5

L

LAN installation 3-16
LED 2-2
light indicators 2-2
limited fabric RSCN 3-12
list
switch binding membership 5-23, 5-29
location 2-3
product 3-10
logging into product 1-8
logical unit number 4-5
login 1-8
loopback diagnostic test 7-7
LUN 4-5

M

maintenance information 7-9
manual
audience xv
conventions xvi
forwarding comments xvii
ordering xviii
organization xv
related xvi
manufacturer 2-4
McDATA
products 10-1
Solution Center xvii
McDATA Fabric 1.0 3-15
McDATA Fabric 1.0 mode 2-13
members of a zone 4-7
membership list
switch binding 5-23, 5-29
menu
configure 3-1
merging
zoned fabrics 4-11
merging zoned fabrics 4-11
mode
interop
defining 3-15
McDATA Fabric 1.0 2-13
Open Fabric 1.0 2-13
model number 2-4
multiswitch fabrics, creating 4-11

N

N_port ID virtualization 9-3
name
community 3-19
FRU 2-11
port 2-5, 2-7
defining 3-3
product 2-3
defining 3-9
naming conventions
zones 4-7
zones and zone sets 4-7
zoning 4-7
node
WWN 2-14
Node List 2-14
nonvolatile random-access memory (NVRAM) 4-7
NPIV
configure 3-7
NPIV view 3-7
NPIV, installing 9-3
number
port 2-5, 2-7, 2-14
NVRAM 4-7

O

Open Fabric 1.0 2-13, 3-16
open system interconnection standards 4-5
OpenTrunking feature, installing 9-3
operating parameters 2-12
Operating Parameters page 2-12

operating speed 2-7
operating state reason 2-8
operational state
    port list 2-6
    port properties 2-8
organization of manual xv
OSI standards 4-5
OSMS 1-2
    enable and disable 3-20

P

parameters
    fabric 3-14
parameters, switch 3-11
part number, FRU 2-11
password
    default 1-3, 1-8, 3-17
    default value 3-2
    dialog box 1-7
    login 1-8
Performance page 2-15
persistent binding 4-5
port
    beaconing 2-8, 7-5
    block configuration 2-8
    blocked 2-8
    blocking 2-5, 3-3
    configuring basic information 3-2
    enable switch binding for 5-31
    list 2-4
    monitoring 2-4
    name 2-5, 2-7
        defining 3-3
    number 2-5, 2-7, 2-14, 3-18
    number in zoning identification 4-8
    numbers
        interoperability mode 4-7
        zone members 4-8
    operational state 2-6
    speed 3-4
    state 2-6
    type 2-6, 2-7
        defining 3-4
    UDP number 3-19
    WWN 2-8, 2-14
    zoning, disadvantages 4-8
port binding
    zoning 4-5
port fencing 3-30
Port List page 2-4
position, FRU 2-11
preferred domain ID 2-12, 3-13
preferred path 3-28
priority
    switch 3-15
priority, switch 2-13
product
    contact 2-3, 3-10
    description 2-3, 3-10
    EC level 2-4
    firmware level 2-4
    identification, configuring 3-9
    IP address 1-7
    location 2-3, 3-10
    manufacturer 2-4
    model number 2-4
    name 2-3
        defining 3-9
    serial number 2-4
    type number 2-4
    view 2-1
    WWN 2-3
publications
    forwarding comments xvii
    ordering xviii
    related xvi

R

R_A_TOV 2-13, 3-14
    setting 3-14
RAID 4-6
rear view 2-2
reason, operating state 2-8
receive BB_Credits 3-5
redundant array of independent disks 4-6
registered state change notification 2-13, 3-11
registered trademarks xviii
related documentation xvi
rerouting delay 2-12, 3-12
    enterprise fabric mode 5-23
Resource Allocation Time Out Value 2-13, 3-14
retrieving dump file 7-9

RSCN 3-11
domain 2-13
enable 3-12
limited fabric 3-12
suppress 2-13
suppress after IPL 3-12
suppress on zoning change 3-12
suppress zone set activation messages 3-12
RSCNs
domain 5-24
Rx BB Credit view 3-5
RX field size 2-14

S

S/390 2-13, 3-15
SAN management
EFCM 10-2
SANavigator 1-7, 10-1, 10-2
fabric planning 10-2
SANtegrity Authentication, installing 9-3
SANtegrity Binding, installing 9-3
SBML
overview 5-23, 5-29
scalability, EFCM 10-2
SCSI connection 4-5
secure shell (SSH) 3-20
secure socket layer 3-21, 3-22
security 5-1
segmented E_Port 2-8, 4-11, 4-12
serial number 2-4
FRU 2-11
server device name 4-5
server-level access, controlling 4-5
service representative xvii
settings
security 5-1
small computer system interface 4-5
SNMP 1-2, 3-9
community name 3-19
configure 3-18
enable and disable 3-18
management stations 3-18
speed
director 2-13
operating 2-7
port 3-4
switch
setting 3-13
SSH
enable and disable 3-20
key 3-20
SSL 3-21
configure 3-22
starting EFCM Basic 1-7
starting to use EFCM Basic 1-6
state
list of operational states 2-6
operational 2-8
port 2-6
statistics
counter 2-15
wraps 2-15
status
FAN 2-8
FRU 2-11
indicators 2-2
storage volume 4-5
storage-level access control 4-6
subnet mask 3-2
setting 3-17
suppress RSCNs on zoning change 3-12
suppress zone set activation RSCN 3-12
switch binding 5-23
online state functions 5-30
switch binding membership list
overview 5-23, 5-29
switch identification 3-9
switch parameters view 3-11
switch priority 2-13, 3-15
switch speed
setting 3-13

T

tasks
EFCM Basic 1-2
technical support xvii
telnet 3-20
terminology
key 1-5
user interface 1-10
test port 7-7
time 3-10

time fields 3-10
trademarks xviii
trap message recipients 3-18
trap recipient 3-18, 3-19
type
    port 2-6, 2-7
        defining 3-4
type number, product 2-4

U

UDP port number 3-18, 3-19
unblocking a port 2-8
upgrade firmware 7-13
user datagram protocol port numbers 3-18
user name 1-8
    default 1-3, 1-8, 3-17

V

version
    FA MIB 3-18
view
    front 2-2
    rear 2-2
viewing
    hardware 2-1
    operating parameters 2-12

W

web browser 1-7
web browser level 1-3
wraps, definition 2-15
write authorization 3-19
WWN 2-3
    attached port 2-8
    interoperability mode 4-7
    node 2-14
    port 2-8, 2-14
    zone members 4-7
    zoning identification 4-7

Z

zone
    definition 1-5
    overview 4-7
zone FlexPars 3-12
zone members
    definition 1-5
    interoperability mode 4-7
    maximum number 4-7
    port numbers 4-8
    types 4-7
    WWNs 4-7
zone set
    activating 4-17
    active 4-10
    deactivating 4-17
    definition 1-5
    description 4-9
    naming conventions 4-7
    suppress RSCN on activation 2-13
zoned fabrics, merging 4-11
zones
    description 4-7
    identifying by port number 4-8
    identifying by WWN 4-7
    naming conventions 4-7
zoning 4-13, 4-14, 4-17
    by port 4-8
    concepts 4-6
    configurations
        compatibility 4-11
    controlling access 4-2
    disabling 4-10
    identification by WWN 4-7
    multiple products, illustrated 4-4
    naming conventions 4-7
    overview 4-1
    single product, illustrated 4-3